

In The Matter Of:
United States vs.
PFC Bradley E. Manning

Vol. 6
June 12, 2013
UNOFFICIAL DRAFT - 6/12/13 Afternoon Session

Provided by Freedom of the Press Foundation

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21

VOLUME VI

IN THE UNITED STATES ARMY

UNITED STATES

VS.

MANNING, Bradley E., PFC COURT-MARTIAL

U.S. Army, xxx-xx-9504

Headquarters and Headquarters Company,

U.S. Army Garrison,

Joint Base Myer-Henderson Hall,

Fort Myer, VA 22211

_____ /

The Hearing in the above-titled matter

was continued on Wednesday, June 12, 2013, at 1:30

p.m., at Fort Meade, Maryland, before the Honorable

Colonel Denise Lind, Judge.

DISCLAIMER

This transcript was made by a court reporter who is not the official Government reporter, was not permitted to be in the actual courtroom where the proceedings took place, but in a media room listening to and watching live audio/video feed, not permitted to make an audio backup recording for editing purposes, and not having the ability to control the proceedings in order to produce an accurate verbatim transcript.

This unedited, uncertified draft transcript may contain court reporting outlines that are not translated, notes made by the reporter for editing purposes, misspelled terms and names, word combinations that do not make sense, and missing testimony or colloquy due to being inaudible by the reporter.

1 APPEARANCES:

2
3 ON BEHALF OF GOVERNMENT:

4 MAJOR ASHDEN FEIN

5 CAPTAIN JOSEPH MORROW

6 CAPTAIN ANGEL OVERGAARD

7 CAPTAIN HUNTER WHYTE

8 CAPTAIN ALEXANDER Von Elten

9
10 ON BEHALF OF ACCUSED:

11 DAVID COOMBS

12 CAPTAIN JOSHUA TOOMAN

13 MAJOR THOMAS HURLEY

INDEX

June 12, 2013

WITNESS: SPECIAL AGENT DAVID SHAVER	Page
CONTINUED REDIRECT	7
WITNESS: GREGORY WEAVER	
DIRECT EXAMINATION	21
CROSS EXAMINATION	52
REDIRECT EXAMINATION	60
RECROSS EXAMINATION	61
WITNESS: MARK KITZ	
DIRECT EXAMINATION	66
CROSS EXAMINATION	83
REDIRECT EXAMINATION	99
COURT EXAMINATION	101
RECROSS EXAMINATION	104
REDIRECT EXAMINATION	106

INDEX (Continued)

June 12, 2013

1	WITNESS: CAPTAIN THOMAS CHEREPKO	Page
2	DIRECT EXAMINATION	110
3	VOIR DIRE	119
4	DIRECT EXAMINATION	122
5	VOIR DIRE	124
6	DIRECT EXAMINATION	129
7	CROSS EXAMINATION	145
8	REDIRECT EXAMINATION	178
9	COURT EXAMINATION	180
10	CONTINUED REDIRECT	183
11	CONTINUED RECROSS	184
12	CONTINUED REDIRECT	185
13	WITNESS: JASON MILLIMAN	
14	DIRECT EXAMINATION	186
15	CROSS EXAMINATION	202
16	COURT EXAMINATION	221

1 PROCEEDINGS,

2 THE COURT: Court is called to order. Let
3 the record reflect all parties present when the court
4 last recessed are again present in court. Court is
5 called to order.

6 Are there any issues we need to address?

7 MR. FEIN: No, ma'am.

8 THE COURT: Call your next witness.

9 MR. COOMBS: No, ma'am.

10 MR. FEIN: Ma'am, the United States offers
11 two stipulations, Prosecution Exhibit 117 and
12 Prosecution Exhibit 119.

13 Your Honor, first Prosecution Exhibit 117
14 Chief Warrant Officer Jon LaRue.

15 (Whereupon, Prosecution Exhibit 117,
16 stipulated testimony of Chief Warrant Officer Jon
17 LaRue, was read into the record.)

18 MR. FEIN: Your Honor, the stipulated
19 testimony of Jacqueline Scott dated June 10, 2013.

20 (Whereupon, Prosecution Exhibit 119,
21 stipulated testimony of Jacqueline Scott, was read into

1 the record.)

2 MR. MORROW: United States recalls Special
3 Agent David Shaver.

4 Whereupon,

5 SPECIAL AGENT DAVID SHAVER,
6 called as a witness, having been previously duly
7 sworn to tell the truth, the whole truth, and
8 nothing but the truth, was examined and testified as
9 follows:

10 CONTINUED DIRECT EXAMINATION:

11 Q Agent Shaver, you are still under oath.

12 A Yes, sir.

13 Q Agent Shaver, what is a SAM or SAM file?

14 A Sir, that is a systematic, systematic
15 assist manager. What that is, part of the Microsoft
16 security. It is a file within XP operating system. It
17 contains both the user names and part of the encrypted
18 password.

19 Q Now, what do you mean by part of the
20 encrypted password?

21 A Sir, I'll explain it. I'll explain how.

1 Q Okay. Take your time.

2 A Encrypted works. When you log into a
3 computer you type your password in. It's plain text.
4 You can see it.

5 Well, what the computer does is it takes
6 that plain text password and passes it through a
7 mathematical algorithm and creates a hash value. This
8 is a first step of a security feature. Storing
9 passwords in plain text is not very smart. Bad people
10 can get them very easily. It as hash value and breaks
11 it up into two parts, part goes to the SAM file and
12 part of it goes to the system file.

13 This is another security feature to have
14 the password, the hash and password broken up into two
15 pieces and finally when the computer is running the
16 system files, the SAM and system files are locked,
17 whereas a normal user cannot access them.

18 Q Now, what users of a computer could access
19 the system file and SAM file?

20 A You would have to have administrative level
21 privileges.

1 Q If you don't have administrative level
2 privileges what is another way you can view the SAM or
3 system file?

4 A You could recruit the boot and use Linux
5 operating system which is a configure to run off of the
6 CD. So it doesn't actually install, it runs from it.
7 Then you can navigate to the SAM or system file and
8 view the contents.

9 Q Let's back up. What do you mean by, so
10 what is Linux first?

11 A Sir, that's just another operating system.

12 Q And what do you mean by booting the
13 computer from a CD?

14 A Well, you first off, you need to download
15 from the internet a Linux distribution. You would burn
16 it from an ISO file which you download and burn it to a
17 CD.

18 Then you would basically, when the computer
19 boots up, you would see like the Dell screen, for
20 example, it may say something press F9 to boot from CD.

21 Q Now, let me stop there. Where would you

1 find the Linux operating system? Free on the internet?

2 A Yes, sir.

3 Q And if you burned a CD with a Linux
4 operating system on it, at least on a MacIntosh or
5 Apple, Macbook Pro, where would you see evidence of
6 that?

7 A That would be the disk utility log file.

8 MR. MORROW: Retrieving Prosecution Exhibit
9 125.

10 I'm handing the witness Prosecution Exhibit
11 125.

12 BY MR. MORROW:

13 Q Agent Shaver, do you recognize that
14 document?

15 A Um --

16 Q Take a couple minutes to review it.

17 A Yes, sir. This appears to be the disk
18 utility log file.

19 Q And did you review this disk utility log
20 file?

21 A Yes, sir; I did.

1 Q When you reviewed it, did you observe any
2 activity that would suggest that a Linux operating
3 system was burned to a CD?

4 A Yes.

5 Q Can you point out multiple places or just
6 one place.

7 (Witness reading.)

8 A There are multiple places, sir.

9 Q What's the first example?

10 A Line 112.

11 Q Okay.

12 MR. MORROW: Permission to publish, Your
13 Honor?

14 THE COURT: Go ahead.

15 BY MR. MORROW:

16 Q I am publishing page 3 of Prosecution
17 Exhibit 125.

18 Agent Shaver, can you explain the
19 information contained in line 112 and below, please?

20 A Sure. Yes, sir. On February 1st, 2010 at
21 1317 hours local time, the burning image, the file name

1 system rescue dash X86-1.3.5 dot iso, it talks about
2 the log file and shows it preparing data for burning.
3 Opening session. Writing session. Closing.
4 Verification. And finally line 129 says burn complete
5 successfully.

6 Q And based on your review of the disk
7 utility log, did you observe or what are the other
8 dates you observed, approximately observed a --

9 A Early March 2010.

10 Q I'm publishing page 8 of Prosecution
11 Exhibit 125.

12 Again, explain the information in line 365.

13 A Sir, can you slide that a little further up
14 so I can see it further down?

15 Q Sure.

16 A Other way.

17 Q Other way.

18 A Yes, sir. Line 365 says on March 2nd, 2010
19 17:48:51 hours burning image system rescue CD dash
20 X86-1.3.5 dot iso. And then at line 382 it shows that
21 the burn completed successful.

1 Q Now, again what is the dot ISO mean?

2 A That's an image file for a CD.

3 Q And how do you know that, just looking at
4 that, how do you know that's a Linux operating system?

5 A I have actually burned this disk to CD and
6 utilized it, viewed the contents.

7 Q Now, let's say that you boot a separate
8 computer using a CD with Linux on it, how would you
9 view the SAM file?

10 A What you do is boot to CD. The operating
11 system would come up. You would have to basically
12 mount the hard drive. Mounting is making it accessible
13 to the Linux operating system. Navigate to the SAM
14 file and you would use a hex editor to view the
15 context.

16 Q What's a hex editor?

17 A To view the contents of Microsoft Word
18 document, you would use the program Microsoft Word.
19 The SAM file is a database. It's a registry file.
20 It's complicated file but a hex editor can view the
21 contents.

1 MR. MORROW: Retrieving Prosecution Exhibit
2 130 for identification.

3 People handing the witness Prosecution
4 Exhibit 130 for identification.

5 BY MR. MORROW:

6 Q Do you recognize those images?

7 A Yes, sir; I do.

8 Q And what are they?

9 A These are two screenshots I created. The
10 first one is of a chat that was recovered from PFC
11 Manning's personal Macintosh. The second is a
12 screenshot of the EnCase program of viewing the SAM
13 file from the dot 22 computer.

14 MR. MORROW: Permission to publish, Your
15 Honor.

16 THE COURT: Go ahead.

17 BY MR. MORROW:

18 Q Can you see that Special Agent Shaver?

19 A Yes, sir.

20 Q Let's start here. Do you see the line that
21 says dawgnetwork and there's a series of numbers and

1 letters 80C1104?

2 A Yes, sir.

3 Q What is that?

4 A That is a hex value, a part of the SAM file
5 from dot 22 or dot 40.

6 Q And how do you know that?

7 A I examined both computers specifically the
8 SAM file but the entire computer and (INAUDIBLE)
9 allocated to find the unique string and it was only
10 located within the SAM file of the dot 22 or dot 40
11 computer.

12 Q Based on the presence of that string of
13 numbers and characters in the chats, what does that
14 tell you?

15 A Somebody had gained access to the SAM file
16 to find that unique string.

17 Q Other than being administrator, is that the
18 only way you would be able to gain access to that
19 string of numbers and letters?

20 A There may be some hacker tools out there
21 but the most common way would be to use a Linux CD to

1 do this.

2 Q Did you verify whether the SIPRNET
3 computers associated with PFC Manning could be booted
4 from a CD?

5 A Yes, sir. I turned it back into a virtual
6 machine.

7 Q Let's stop. What's a virtual machine?

8 A Sir, again a virtual machine would be, your
9 computer would be the host, in my case the Windows
10 machine, but the guest operating system, the virtual
11 machine, could be anything, Linux, Mac, Windows.

12 Q And explain the process of booting that you
13 went through here.

14 A Very simple. I just burned the same system
15 rescue CD that I found on PFC Manning's personal
16 Macintosh computer, burned the CD. Restored the --
17 created the virtual machine and booted the virtual
18 machine from that CD.

19 Q Once you booted the virtual machine, what
20 did you do next?

21 A I then navigated to the SAM file and I was

1 using the hex editor, was able to view the contents.

2 Q And ultimately, why would somebody be
3 interested in the contents of a SAM file? What's
4 contained in that?

5 A Again, users names.

6 MR. HURLEY: Objection. Calls for
7 speculation.

8 THE COURT: Do you know what's in there?

9 THE WITNESS: Yes, ma'am.

10 THE COURT: Overruled.

11 A User names and part of a hash of a
12 password.

13 Q Finally, what's a rainbow table?

14 A Rainbow table. As we talked about,
15 passwords are hash values. That's how they use
16 mathematical (INAUDIBLE) to create hash table. Rainbow
17 table, you regenerate known hash values. So you have
18 dictionary attacks that have already generated hash
19 value and then you have a program that checks it. The
20 passwords, the hash value to see if they match. It
21 would speed up cracking or decrypting passwords.

1 Q And why do you use a rainbow table?

2 A It's, it's faster to decrypt a file, a
3 password. And in this case you have the hash value of
4 a user's account. The rainbow tables would be tailored
5 to attack that and it would take just moments on a good
6 computer to crack a password.

7 Q And in this case the hash value 80C1104,
8 what was that hash value associated with in the SAM
9 file?

10 A That's the thing, sir. In this case, the
11 person who did this only got part of the hash value.
12 It's not quite right. But it appears to be from the
13 user's account FTP user.

14 Q What is the FTP user account?

15 A That's just a user account. It was on both
16 22 and 40 as probably part of the original build that
17 was pushed out. It would just be another local account
18 on the computer.

19 MR. MORROW: Your Honor, move to admitting
20 Prosecution Exhibit 130 into evidence as Prosecution
21 Exhibit 130.

1 MR. HURLEY: No objection, Your Honor.

2 THE COURT: Prosecution Exhibit 130 is
3 admitted.

4 May I see it, please? Thank you.

5 Thank you Agent Shaver.

6 THE COURT: Cross-examination? I'm sorry.

7 MR. MORROW: I'm handing Exhibit 125 back
8 to the court.

9 CONTINUED RECROSS BY MR. HURLEY:

10 Q Good afternoon, Agent Shaver?

11 A Good afternoon, sir.

12 Q Now, you just testified that the hash value
13 that was included in the chat was not the full hash
14 value?

15 A That's correct.

16 Q So in order for a person to actually gain
17 access to the passwords contained in the SAM, they
18 would have needed more of the hash value?

19 A Yes, sir, I mentioned the system file, you
20 would need that part as well.

21 Q So the hash value included in the chat

1 wouldn't be enough to actually gain any passwords or
2 user information?

3 A Correct.

4 MR. HURLEY: No further questions. Thank
5 you.

6 THE COURT: Redirect?

7 MR. MORROW: No, Your Honor.

8 THE COURT: Temporary or permanent excusal?

9 MR. MORROW: Temporary, Your Honor.

10 THE COURT: Once again, you're temporarily
11 excused. Same rules apply.

12 THE WITNESS: Yes, ma'am.

13 MR. FEIN: The United States asks for a
14 10-minute recess. It went a little faster than we
15 planned, just to get the other witnesses.

16 THE COURT: Court is recessed until ten
17 after 1400 or 2:00 o'clock.

18 (Recess taken.)

19 THE COURT: Please be seated. Court is
20 called to order.

21 Major, please account for the parties.

1 MR. FEIN: Yes, ma'am. All parties are
2 present with the exception of Captain Morrow, Captain
3 Whyte and Mr. von Elten are present.

4 MR. Von ELTEN: Ma'am, the United States
5 calls Greg Weaver.
6 Whereupon,

7 GREGORY WEAVER,
8 called as a witness, having been first duly sworn to
9 tell the truth, the whole truth, and nothing but the
10 truth, was examined and testified as follows:

11 DIRECT EXAMINATION BY MR. Von ELTEN:

12 Q Are you Greg Weaver of Bristow, Virginia?

13 A Sir, yes, I am.

14 Q Good afternoon, Mr. Weaver.

15 A Good afternoon, sir.

16 Q What is your military experience?

17 A Sir, I'm a retired noncommissioned officer.

18 I retired in 19*7 as a retired noncombat (INAUDIBLE).

19 Last duty assignment was out of the Pentagon.

20 Q What did you do in your last duty
21 assignment?

1 A In my last duty assignment for the military
2 I was the Army operations center team lead working 24/7
3 operations in the Army op center, directly reporting to
4 the secretary and chief staff of the army.

5 Sir, today I lead a compliance branch team
6 of military and civilian personnel, the compliance
7 branch underneath the compliance division of Army Cyber
8 Command, a newly formed organization to report on
9 compliance activities across the Army.

10 Q What else does that entail?

11 A Sir, predominantly we are the reporting
12 agency for all inspections, all compliance inspections
13 across the Army, the conduct of lessons learned, the
14 computer network defense service providing services
15 associated with our Cyber Mission, plus a number of
16 administrative duties.

17 Q Mr. Weaver, what is information assurance?

18 A Sir, information assurance, the foundation
19 principles of information assurance is a united
20 approach by which we get after the confidentiality,
21 integrity and availability non-(INAUDIBLE) of systems

1 and information systems and information in general to
2 ensure its security and reusability or usability within
3 the Army.

4 It's a, it's not a standalone, not a
5 standalone concept but it incorporates many facets of
6 other security disciplines and not just information
7 assurance.

8 Q What metrics do you use to measure
9 information assurance?

10 A Sir, there's many metrics to measure
11 information assurance. One of them would be compliance
12 inspection. One of them would be reporting,
13 assessments in general, how well an individual or
14 organization is evaluated from an operational
15 standpoint as to how well they perform information
16 assurance, using guidelines, decision, standards,
17 checklists, best practices and so forth.

18 Q How long have you been in this position?

19 A In this position, sir, just over, since
20 November of 2011.

21 Q What position did you hold prior to your

1 current one?

2 A Prior to this I was a contract support to
3 the Department of Defense and the Defense (INAUDIBLE)
4 Information Assurance Program at the DoD CIO's office
5 serving capacity as a subject matter expert in the
6 areas of information assurance, computer network
7 defense and other technology areas associated with
8 policy and procedures.

9 Q How long did you hold that position?

10 A Sir, it was just over 13 months.

11 Q What certifications do you possess?

12 A Sir, currently I am a Certified Information
13 Systems Security Professional and SANS global
14 information assurance certified incident handler.

15 Q What does the CISSP certification mean?

16 A Sir, it's a, it's the top level preeminent
17 security professional, security certification required
18 for information assurance professionals within the DoD
19 and it's an industry recognized certificate for the
20 industry in general.

21 Q Why do you have that certification?

1 A Two reasons. Professional respect and
2 responsibility of the professional so it serves as an
3 indicator of the expertise and secondly it is a
4 requirement within the Army if you maintain an
5 information assurance position to hold such
6 certifications as they are identified by your unique
7 description or position.

8 Q What does your SANS certification signify?

9 A The SANS certification is a longstanding
10 certification I maintained since 2001. It is the
11 certified information, it's a certificate of ability to
12 perform incident response, incident handling for
13 systems and networks that have had an intrusion or
14 event.

15 Basically how to prepare for, respond,
16 react and follow up with any system or network that may
17 have been intruded upon or events that may have
18 occurred on the network.

19 Q How long have you been working in
20 information assurance?

21 A Sir, since 1998.

1 Q What were you doing when you began working
2 in information assurance?

3 A Sir, when I began I originally started in
4 this career field after I retired from the service. I
5 was a team member of the Army Computer (INAUDIBLE)
6 Response Team, contractor support in support of the
7 Army's cert standing out and formalizing a brand new
8 organization to establish computer emergency response
9 processes within the Army and across the five theaters
10 that we had at the time and their cert procedures and
11 then as well as or reporting to and supporting the
12 Department of Defense, DoD, DIS and at the time JTFC
13 and now Cyber Command.

14 Q Let's talk about AR25.

15 A Yes.

16 Q Are you familiar with it?

17 A Yes.

18 Q How?

19 A In 2002 I began work with the Army CIOG6 by
20 leaving the Army computer emergency response team and
21 went to the Army CIOG6. My primary duties and

1 responsibilities when I got there was the authoring of
2 AR25-2 and then predominantly was the sole author and
3 responsible for creating, staffing, collaboration and
4 eventually publication of AR25-2.

5 Q What version did you write?

6 A The initial version it was published in
7 2003 and then the two subsequent versions in 2007 and
8 then the rapid action revision in 2009.

9 Q And how many versions are there?

10 A Currently 2009 rapid action revision is the
11 current 25-2.

12 Q What was the first version?

13 A It was just information assurance 25-1
14 dated 2003.

15 Q How long did you spend drafting AR25-2?

16 A I spent approximately nine months of
17 dedicated effort to creating and drafting the
18 regulation from the DoD and Army directives at the
19 time.

20 Q What other documents related to AR25-2 have
21 you drafted?

1 A I've helped direct authorship of
2 approximately best business practices over the course
3 of about four years in 2003 to 2007. Either the
4 principal author or co-author of best business
5 practices.

6 Q What is AR25-2?

7 A Sir, AR25-2 establishes the standards and
8 processes and procedures by which regulatory
9 requirements of Army efforts to instill or to apply
10 information assurance practices for the network
11 security across the Army.

12 Q To whom does AR25-2 apply?

13 A Sir, it applies to everybody and if you sit
14 or -- it applies to all users. Obviously applicable to
15 who are responsible for filing AR25-2, commanders,
16 designating accredited officials are required to follow
17 the rules and policies associated with AR25-2 and the
18 design of their systems and incorporate IA principals
19 in the policy, Army Reserve, National Guard, medical
20 community, Corps of Engineers and so forth. Applies to
21 everybody within the Army.

1 MR. Von ELTEN: I'm retrieving Prosecution
2 Exhibit 95 for identification.

3 THE COURT: Come on up.

4 BY MR. Von ELTEN:

5 Q Handing it to the witness.

6 A Thank you.

7 Q Do you recognize that document, Mr. Weaver?

8 A Yes I do sir. It's AR25-2.

9 Q What is it?

10 A It's a rapid action revision dated
11 March 23, 2009.

12 Q How do you recognize it?

13 A It is the format by which the Army
14 publishes Army regulations. This one is in single page
15 format.

16 MR. Von ELTEN: Ma'am, the United States
17 offers Prosecution Exhibit 93 for identification.

18 THE COURT: (INAUDIBLE) is this something I
19 took judicial notice of?

20 Are they already admitted or are we
21 admitting them now?

1 MR. FEIN: Ma'am, they have not been
2 separately marked at all. Although we have taken
3 judicial notice and the government has the consolidated
4 list for the court and has not given that to the court
5 yet. But none of the items have been printed or
6 marked.

7 THE COURT: Any objection, Defense?

8 MR. HURLEY: No, ma'am.

9 THE COURT: Thank you. May I see it,
10 please?

11 Prosecution Exhibit 93 is admitted.

12 MR. Von ELTEN: Retrieving it from the
13 witness.

14 BY MR. Von ELTEN:

15 Q Mr. Weaver, let's talk about the acceptable
16 use policies.

17 A Yes, sir.

18 Q What is an acceptable use policy?

19 A Sir, an acceptable use policy is mandated
20 by DoD for all users to acknowledge and comply. It's a
21 signature, with a signature. It outlines the

1 procedures and the policies associated with appropriate
2 use of government systems and on a government network
3 or system in general as provided by the government to
4 outline the standards and outline the standards by
5 which users are held accountable to conduct and
6 behavior while on or operating with that system.

7 MR. Von ELTEN: Permission to publish,
8 ma'am.

9 THE COURT: Go ahead.

10 BY MR. Von ELTEN:

11 Q Mr. Weaver, do you recognize this section?

12 A I do, sir.

13 Q What is it?

14 A This is one of the subparagraphs --

15 THE DEFENSE: We're going to object based
16 on relevance. PFC Manning is charged with violating
17 specific sections of 25-2. This is not one of these
18 sections.

19 THE COURT: Where are you going with this?

20 MR. Von ELTEN: To establish the framework
21 by which 25-2 establishes acceptable uses.

1 THE COURT: Is this going to be a long
2 discussion?

3 MR. Von ELTEN: No, ma'am.

4 THE COURT: All right. I'll overrule the
5 objection. Go ahead.

6 BY MR. Von ELTEN:

7 Q What does the acceptable use policy do?

8 A So, sir, what you see here is the wording
9 manner that is prescribed as a requirement to access
10 any information system. It is the warning banner that
11 is part of the display of any users' access to
12 information and the users agreement outlines the
13 standards by which that access is also permitted in
14 addition to the warning banner.

15 THE COURT: Captain von Elten, what pages
16 of the regulations am I looking at?

17 MR. Von ELTEN: 26.

18 THE COURT: Thank you.

19 BY MR. Von ELTEN:

20 Q What uses does it authorize?

21 A That the AUP outlines the appropriate use

1 of the information system other than or in addition to
2 the additional authorized use of that, of that system
3 for conduct of government business. This warning
4 banner also outlines that there's no expectation of
5 privacy with that, with the exception of that which is
6 already controlled by other policies such as legal or
7 medical restrictions.

8 Q How are government means (sic.) determined?

9 A Means?

10 Q Government needs determined?

11 A Usually by the commissioner, by the command
12 or by the organization that owns that system or has
13 accredited that system for use decides or determines
14 what that need is, sir.

15 Q Are AUPs required?

16 A They're required.

17 Q How long have they been required?

18 A Since that Regulation 25-2. This version
19 was a rapid action revision because of the requirement
20 by DoD to change the mandate, the acceptable use. So
21 in 2009 this RAR was published.

1 Q Why are AUPs used?

2 A The AUPs are basically an agreement between
3 the government or the organization and the user.

4 The user signs it understanding that the
5 rules and responsibilities they have on that network
6 are the rules and responsibilities that they have in
7 the performance of their duties as well as acknowledge
8 their responsibility and when authorized, when you can
9 use the government system for nonofficial use.

10 However, but it's still authorized such as
11 NWR support or e-mail to a user, civilian web mail or
12 something like that.

13 Q What does AR paragraph 1-5J prohibit?

14 A Sir, 1-5J prohibits or specifically
15 prohibits actions and functions within the Army
16 associated with the use of information systems and IA
17 principles.

18 Q What are code examples?

19 THE DEFENSE: We're going to object again.
20 This man is not charged with violating that division of
21 AR25-2.

1 THE COURT: Then why are we discussing it?

2 MR. Von ELTEN: Establishing framework,

3 Your Honor. My last question.

4 THE COURT: All right. Go ahead.

5 A Your question again, sir?

6 Q A few examples. What are a few examples of
7 activities prohibited in 1-5J?

8 A So those violations are covered in the
9 regulation in bolded text throughout the regulation
10 specifically. Some violations would be unauthorized
11 use of the system, installing or downloading or
12 accessing information, installing or downloading
13 software, accessing information which is outside the
14 control or boundaries of authorized use, failure to
15 scan systems for malicious content, uploading
16 personnel, personnel files or personal content that is
17 not DoD related.

18 Q Let's talk about information assurance
19 training.

20 A Sure.

21 Q Are you familiar with information assurance

1 training?

2 A I am.

3 Q How are you familiar with it?

4 A Both as a user I am required by the same
5 policy to take training every year and as a SME for IA
6 within the Army I've contributed to some of the content
7 associated with the initial versions of the information
8 assurance training.

9 Q What policies required IA training?

10 A The AR25-2 requires training on an annual
11 basis. DoD also requires as part of their policies
12 that all users within the Department of Defense
13 conducting information assurance training annually.

14 Q How does a user complete his obligations to
15 complete information assurance training?

16 A Both the Army and the DoD have instituted
17 online CPT based, computer based training, so it's
18 accessible through the web. So it's very easy to
19 accomplish.

20 Q What does it take to accomplish that?

21 A Log on with the website, go through the

1 scenario-driven computer based training. You have a
2 certificate at the end of it that you digitally sign or
3 print it out and sign.

4 Q What does it take to earn that certificate?

5 A Completion of the training, sir.

6 So you have to answer at least 10 questions
7 or 20 questions, I'm not sure what it is at the end of
8 the test and you obviously have to pass or you have to
9 do it again.

10 Q And how long has this training been
11 required?

12 A The training within the Army has been,
13 since before 2009 when DoD instituted the DoD level
14 training, the Army adopted the DoD training and just
15 used that as a standard.

16 Q What work did you do in developing IA
17 training?

18 A So prior to the DoD integration --

19 THE COURT: Yes?

20 THE DEFENSE: Your Honor, we object on
21 relevance and we would also ask the judge to take

1 judicial notice of DoD IA training as completed it a
2 number of times.

3 THE COURT: Where are we going with this?

4 MR. Von ELTEN: Ma'am, United States is
5 offering this for evidence of PFC Manning's knowledge
6 because he completed IA training and we're going to
7 discuss the contents of the training he would have
8 completed.

9 THE COURT: Which of these specifications
10 has a knowledge element?

11 MR. Von ELTEN: Ma'am, the 104
12 specification requires knowledge. He did complete the
13 training.

14 THE COURT: This training is relevant to
15 the 104 specification?

16 MR. Von ELTEN: Yes, ma'am.

17 THE COURT: All right. Make it -- go ahead
18 and make it, make it brief on this portion, okay.

19 MR. Von ELTEN: Yes, ma'am.

20 I'm retrieving Prosecution Exhibit 7.

21 THE COURT: Overruled.

1 BY MR. Von ELTEN:

2 Q Mr. Weaver, do you recognize these CDs?

3 A Yes, sir. These are two DoD information
4 assurance IA training CDs by DoD and downloadable.

5 It's also, you can order through the DoD for use
6 remotely or as needed by users. So this is also an
7 acceptable way to do the training.

8 Q What versions are they?

9 A 2000 -- Version 7 and Version 8.

10 Q And how do you recognize those?

11 A Sir, they're identified by the version
12 number at the bottom corner of the CDs.

13 Q How do you know the contents of the CDs?

14 A The contents of the CDs are basically the
15 web pages in the CD format. They're the same IA
16 training that was applicable at the years or the
17 versions these were published.

18 Q Have you seen those CDs used?

19 A Yes, sir, I have. I have a copy of my own.

20 Q With those specific CDs?

21 A The Version 8, yes, sir.

1 MR. Von ELTEN: Ma'am, United States
2 offers -- it's already been, sorry.

3 BY MR. Von ELTEN:

4 Q What kind of threats does that information
5 assurance cover, the training?

6 A Sir, the IA training, it covers a multitude
7 of issues. One of them being user training, user
8 password, security. Security classified information.
9 Army phishing or phishing threats, general threats in
10 particular through a variety of different methods that
11 users might be suspect to or receive e-mail threats,
12 viruses, malware and so forth.

13 Q What kind of outside threats are identified
14 in the training?

15 A Specifically, some of the outside threats
16 would be just factors, trying to do phishing attacks or
17 other similar attempts to gain access networks through,
18 through malware or digital e-mail or phishing, calling
19 you up on the telephone. So both physical security and
20 technical security or IT security.

21 MR. Von ELTEN: Retrieving Prosecution

1 Exhibit 7. Returning this to the court reporter.

2 BY MR. Von ELTEN:

3 Q Let's talk about some of those IA threats
4 you identified.

5 Let's talk about the bad content in
6 particular.

7 MR. VonElten: Permission to publish, Your
8 Honor?

9 THE COURT: Go ahead.

10 BY MR. Von ELTEN:

11 Q This is page 22, Prosecution Exhibit 93.
12 Do you recognize this, Mr. Weaver?

13 A Yes, I do, sir.

14 Q What does paragraph 4-A3 prohibit?

15 A Sir, 4-A3 prohibits the modification of
16 information system for the software to use it for any
17 manner other than intended purpose or added user
18 configurable or unauthorized software such as and not
19 limited to instant messaging, commercial internet chat,
20 (INAUDIBLE) environments where you allow your system to
21 be used by somebody else and those are descriptive in

1 nature or examples, not all inclusive.

2 Q What is the purpose of the prohibition?

3 A Sir, the intent of this prohibition was to
4 prevent, clearly identify the prohibition of users
5 without proper authority to add application software or
6 other content to assist by which is not accredited and
7 processed.

8 Q And who has the authority to make those
9 changes?

10 A Sir, the authorities to make those changes
11 would be an authorized system administrator who has been
12 given the responsibility to change that system for
13 compliance to vulnerabilities or patching as it's known
14 or a DAA, designating accrediting authority, who has
15 determined the appropriate software that's authorized
16 to be installed on a network or on a system by which
17 users can use that piece of application or piece of
18 software.

19 And then commander obviously has some of
20 that responsibility as well.

21 Q What kind of modifications are prohibited?

1 A Sir, there's a number of modifications that
2 are prohibited. Usually anything that the user would
3 do that would violate the integrity of the system is
4 prohibited.

5 And the installation of unauthorized or
6 unaccredited software for which no risk analysis has
7 been done or no acceptance of that risk has been done,
8 that would be prohibited.

9 Sharing the information or sharing your
10 computer information or at the time user ID and
11 passwords with another individual would be prohibited
12 action as well. Sir, that's just --

13 Q Just broadly, what is the process for
14 adding software?

15 A For a, for a user or for --

16 Q For a user.

17 A So for a user, sir, the process would be if
18 you've identified a need, you would ask your IT support
19 specialist, whoever that might be, your system or
20 network administrator, your supervisor, justifying the
21 requirement that you have a requirement to fulfill and

1 you don't necessarily get to dictate the solution, you
2 dictate or you ask for the requirement and allow the
3 system network administrators, the ID, the commander
4 and the DAA to determine the method by which the
5 requirement is filled.

6 So users don't specify, normally don't
7 specify a specific use of a piece of software. They
8 can make recommendations but it's still the
9 determination of the commander.

10 Q What defines the limits of a user's
11 authorization to use a government information system?

12 A The limit is imposed by obviously his duty,
13 his responsibility associated with why he needs access
14 to the system or limited access to the system and/or
15 his responsibility associated with that action or maybe
16 part of his job and requires access to information
17 technology on the daily occurrence of his mission.

18 Q Who determines the parameters of the
19 mission?

20 A Commanders establish the parameters and
21 supervisors where they may fall in, establish those

1 parameters.

2 Q Whose account is a user allowed to use?

3 A Only to be used by the user.

4 Q What permission levels does a user normally
5 receive?

6 A Generally permission of a normal user is
7 basically read accessibility to use a system as it was
8 configured with whatever permissions or roles that the
9 system has or they use it like the applications like
10 Microsoft Office ability to create work files, to
11 create Excel spreadsheets and so forth. So he or she
12 has been given those roles and responsibilities to use
13 the technology as it was designed or as it was
14 provided.

15 Q Let's talk a little bit about insider
16 threats.

17 A Yes, sir.

18 Q What is paragraph AR25-2 paragraph 4-5A4C?

19 A So the, this paragraph outlines the
20 prohibition by normal users or those not authorized to
21 conduct this activity to bypass or circumvent the

1 security parameters that's been installed or part of a
2 operation or part of the design of the system.

3 Q How does a user bypass those mechanisms?

4 A Traditionally as a incident he would have
5 to or she would have to install or modify the system in
6 some way in order to allow them to elevate the
7 privileges on that computer so they can gain access to
8 the box at a higher level or privileged level or, you
9 know, somebody has granted them unauthorized access.

10 Q What are a couple of ways a user could
11 bypass those mechanisms?

12 A So there's a number of ways. One would be
13 obviously to install a piece of software or application
14 or coding that would change the authorization level of
15 his system. Another way would be to find applications
16 or capabilities that would elevate his privileges
17 without changing the access control process and
18 enabling him to do more than he would be authorized to
19 do, or coerce somebody to change it for him, you know,
20 as a friend or as a unauthorized action or part of the
21 system network demeanor to grant him --

1 Q What effect would using a bootable CD have?

2 A A bootable CD could have numerous effects.
3 It depends upon how the CD was written or crafted.

4 Obviously could quickly change the access (INAUDIBLE)
5 controls of the user giving him elevated privileges.

6 Q What if the bootable CD used a different
7 type of operating software?

8 A It's feasible to get access to the system
9 such so that it would circumvent the security and
10 controls of the (INAUDIBLE).

11 Q Mr. Weaver, what tools can be automated on
12 a computer system?

13 A What tools can be automated?

14 Q Yes, sir.

15 A Pretty much anything you want to do on a
16 computer system could be automated if you had the right
17 tools to craft the software or application to do
18 whatever you needed to do.

19 Q What tools can a user add to automate a
20 process?

21 A Sir, what tools can a user add to automate

1 a process surrounding those tools by which he has
2 access to, for example Excel. He would automate the
3 extraction or the publication of content from a
4 spreadsheet for example on a regular basis. Or other
5 tools that might be that allows the automation to occur
6 in an automated manner. It does not equate to his
7 ability to install applications or software which would
8 automate those tasks for him without the system network
9 administrator giving that approval or DAA giving that
10 approval to do that.

11 Q Mr. Weaver, are you familiar with Wget?

12 A I am vaguely familiar, yes.

13 Q How does it work?

14 A As I understand, Wget is basically an
15 application that allows you to download files or do
16 entire content downloading of a website and/or an FTP
17 site in an effort to gather all the information from
18 that site, basically mirroring a site, copying the
19 whole site local to a local drive or whatever.

20 Q When is a user allowed to add Wget?

21 MR. TOOMAN: Your Honor, we'll object to

1 personal knowledge of Wget.

2 THE COURT: What are you objecting about?
3 The witness said he was familiar with it.

4 MR. TOOMAN: Well, like, we would like to
5 explore how the witness is familiar with Wget and the
6 extent of the familiarity.

7 THE COURT: You can do that on
8 cross-examination.

9 BY MR. Von ELTEN:

10 Q Mr. Weaver, what does paragraph 4-17A
11 state?

12 A I don't have that one memorized, sir.

13 Q Is there anything that can refresh your
14 memory?

15 A Just the leading sentence, sir.

16 THE COURT: Why don't you publish it.

17 MR. Von ELTEN: Okay.

18 A Sorry, I don't have them all memorized. I
19 used to but not anymore.

20 So your question again sir, I'm sorry.

21 Q What is the purpose of paragraph 4-17A?

1 MR. TOOMAN: We'll object to the relevance.
2 Again PFC Manning is not charged with violating 4-17.

3 THE COURT: Where are you going with this?

4 MR. Von ELTEN: Ma'am, going with this that
5 the user of the government system has a personal
6 responsibility to follow the rules and this is an
7 example of the rule.

8 THE COURT: Are we going to go through
9 every paragraph?

10 MR. Von ELTEN: Ma'am, this is the last
11 paragraph.

12 THE COURT: It is?

13 MR. Von ELTEN: Yes, ma'am.

14 THE COURT: Okay. Keep it that way.

15 A So to answer your question, sir, this
16 paragraph allows responsibility associated with
17 protecting media, retrieving or inserting from the
18 information system, or any removable media or CD is
19 inserted and removed from a classified system should be
20 treated as such until such time it is properly cleared
21 by the appropriate person or personnel.

1 Q How does personal responsibility affect
2 implementation of AR25-2?

3 A The users are INAUDIBLE), the base, the
4 person with responsibilities for conduct of security
5 information and information systems relies upon the
6 user to do the right thing many times.

7 Technology is advancing rapidly. Policy
8 doesn't always keep up with the technology. So with
9 the guidance of the user, the user has the
10 responsibility and it's entrusted to him and not to
11 exceed the authorities and not exceed their permission
12 and to protect that information and any information
13 systems by, that they do business on and to report any
14 anomalies or violations that they may see to their
15 appropriate security officials.

16 Q Mr. Weaver, when is the user allowed to
17 install Wget?

18 A Never, sir. That user wouldn't have those
19 permission.

20 MR. Von ELTEN: Returning Prosecution
21 Exhibit 93 to the court reporter.

1 Nothing further.

2 THE COURT: Cross?

3 MR. TOOMAN: Yes, ma'am.

4 CROSS-EXAMINATION BY MR. TOOMAN:

5 Q Good afternoon, Mr. Weaver.

6 A Good afternoon, sir.

7 Q Mr. Weaver, do you know what an executable
8 file is?

9 A Yes, sir.

10 Q What is it?

11 A It's a, an executable file would allow for
12 a program application to run its directions or
13 instructions by the system that would execute that file
14 or program, instructions.

15 Q Okay. Do you know whether or not the S2
16 section of PFC Manning's unit, C210 Mountain Division,
17 do you know whether or not they permitted executable
18 files to be run on their --

19 A I do not know that answer.

20 Q Sir, you talked a little bit about the IA
21 training and threats that are discussed within that

1 training. Is al-Qaeda discussed specifically in that
2 training?

3 A There are, the foreign threats, sir, are
4 discussed in the current versions of the training. I
5 don't remember if it was in previous versions but they
6 do talk to -- usually state your foreign actors in the
7 training so, you know just another series of bad guys.

8 Q Okay. To the extent you can remember those
9 past versions, are those foreign groups just grouped
10 generally or are they specifically listed?

11 A They are specifically listed by activists,
12 activists, hacker, insider threat, foreign state. So
13 there's a number of them. I don't remember the exact
14 numbers. There's a group.

15 Q So those are broad categories, they don't
16 get specific for, example, and say al-Qaeda?

17 A No, that would cross some of the boundaries
18 of potentially classified or extremely sensitive
19 information. Obviously the CDs are not designed for
20 those.

21 Q So based on that answer, I assume that they

1 don't specifically mention al-Qaeda in the Iranian
2 peninsula either?

3 A I don't believe they do.

4 Q And you would say that the IA training also
5 doesn't discuss whether or not specific groups use the
6 internet, particular internet sites?

7 A I -- so as a general user you probably
8 would not make that inference as an IA guy with access
9 to classified. You could say that's easily seen in the
10 videos.

11 Q But the training doesn't say al-Qaeda uses
12 WikiLeaks?

13 A No.

14 Q Or al-Qaeda uses ESPN.com?

15 A Not that I know of, no, sir.

16 Q Now, you talked about AR25-2 and the
17 punitive paragraphs and the purpose of AR25-2 was to
18 give some teeth to the IA regulation, correct?

19 A That is a true statement. Yes, sir.

20 Q And while its intention was to give teeth
21 you would also say that AR25-2 is open to

1 interpretation?

2 A As all regulations are, sir. They are open
3 to interpretation, yes, sir.

4 Q And indeed AR25-2 from your view is a
5 regulation that really, the decisions about what's
6 authorized and what's not authorized should be made at
7 the unit level, correct?

8 A No, sir. I disagree. The AR25-2 redlines
9 standard Army practices and principles by which a IA
10 should be conducted understanding it is a part of the
11 antisecurity domain, not just a piece of the security
12 functions. It incorporates, you know, the guidance and
13 the responsibility that it's not just one thing.

14 Q So AR25-2 sort of provides a baseline
15 standard?

16 A Yes, sir.

17 Q You would agree, though, that a commander
18 in a unit could deviate from AR25-2?

19 A A commander by his position would have the
20 authority to do so but he would do so with the advice
21 and understanding of his security staff, his G6 staff,

1 his intelligence staff. It's not a decision he would
2 execute unknowingly or without merit and he could still
3 be subject to a higher level authority which he would
4 have to rescind that authorization.

5 Q So the individual would consider kind of
6 the pros and cons and if they deviated from AR25-2 they
7 would assume some risk?

8 A Yes, sir. But in my experience that risk
9 is usually surfaced at a higher level to ensure that it
10 doesn't impose a greater risk across the enterprise or
11 across the Army. So in my experiences dealing with
12 exceptions or waivers to AR25-2 it is always done in
13 concert with the commander and not solely by the
14 commander. He makes those decisions with the advice of
15 not only the local staff but higher core staff and many
16 times at the Army level.

17 Q You would agree that a deviation from
18 AR25-2, if there were a deviation and a commander or a
19 supervisor had approved it, you wouldn't hold an
20 individual responsible under AR25-2 in a situation
21 where the chain of command had said it's okay for you

1 to do that?

2 A I'm not sure of the question. The
3 command -- so if the user, if the user followed due
4 process and requested the appropriate action and the
5 leadership has approved that action, then it's the
6 leadership's responsibility obviously to manage and
7 monitor that action or request.

8 Q So if a junior soldier was told by his
9 supervisor or his chain of command that something was
10 allowed, you would expect the junior soldier to rely
11 upon the chain of command?

12 A Yes, sir.

13 MR. TOOMAN: One moment, please.

14 BY MR. TOOMAN:

15 Q Mr. Weaver, what is your understanding as
16 to whether or not music would be permitted to be stored
17 on a system?

18 A You want the regulation answer or my
19 opinion, sir?

20 Q Let's go with the regulation answer.

21 A Okay.

1 (Laughter.).

2 A So the answer would be there should be a
3 process in place by which a commander authorized those
4 activities or actions for which they would support WMOR
5 or health and welfare and morale associated with his
6 environment. It is not arbitrary do as you want to do
7 or do whatever you want to do process. It should be
8 requested.

9 It should be a process by which it is
10 approved and the manner in which it is approved is
11 followed every time and obviously enforced when it is
12 not followed.

13 Q Sure. So a commander, if authorizing
14 music, would go through the process that you described.
15 But the language of 25-2 wouldn't allow for music to be
16 stored on a system, correct?

17 A The intent of AR25-2 is not to allow music
18 on a network due to the fact that it's copyright laws
19 for one and secondly it is potentially wrought with
20 malware on the CDs that you would upload from.

21 Q You said the same is true of games?

1 A Yes, sir. Absolutely.

2 Q What about executable files?

3 A Absolutely.

4 Q Now, let's go into, that was the regulation
5 answer. What's the reality?

6 A So the reality is commander has a
7 responsible for health and welfare of his networks and
8 of his soldiers. So as such, there should be a policy
9 or opportunity by which it is done correctly in
10 mitigating the risk associated with those activities.

11 The copyright problem aside, there are
12 technically feasible ways by which your infrastructure
13 guys and security guys and/or gals, I apologize to the
14 ladies in the room, sorry, and your security folks can
15 implement those control measures to mitigate the risk
16 associated with that kind of service. Or outright
17 prohibit look at alternatives to satisfy the
18 requirement if they have one.

19 MR. TOOMAN: Thank you, Mr. Weaver.

20 THE COURT: Redirect?
21

1 REDIRECT EXAMINATION BY MR. Von ELTEN:

2 Q Mr. Weaver, what's the difference between
3 introducing a system and storing a system or storing a
4 file and introducing a file to a system?

5 A Storing a file is anything, it encompasses
6 a number of things. One, where the file was originally
7 created or stored, moved, like a file server or a
8 location by which you, a user had access to, copying
9 from your C drive to a network drive, for example.

10 Introducing a file or executable would be
11 not necessarily something that would be execute --
12 would be installation through a software -- I'm sorry,
13 through a hardware, USB token or a CD or downloading a
14 file that has dutiable in it that would change the
15 configuration of the system or had malicious conduct or
16 intent mind that system itself.

17 So I'm not sure if I answered your
18 question.

19 Q Are the two treated differently under 25-2?

20 A Yes, sir.

21 Q How are they treated?

1 A So the user, so a file on a network or
2 creation of a file on a network and moving documents
3 and so forth would be authorized. Traditionally users
4 do not have the authority -- users do not have the
5 authority to do executable files. That's what system
6 and network administrators are for, people that are
7 trained to understand the impact of what many
8 variations or executables are and the impact to them.
9 Why malware is bad, why CDs are bad because they could
10 contain malicious content, executables, not just the
11 files, the music that's on that CD, for example.

12 MR. Von ELTEN: Thank you.

13 MR. TOOMAN: No, ma'am.

14 THE COURT: I have a couple of questions.

15 EXAMINATION BY THE COURT:

16 Q Is the administrator privilege and user
17 limitations, are they consistent throughout the Army?

18 A The standard, yes, ma'am. Yes, they are.

19 Q So did I understand your testimony that a
20 user of a Department of the Army computer could not
21 load Wget on that computer?

1 A If configured correctly, that would be a
2 true statement, ma'am. You, as a user, cannot load
3 Wget on that system. You would not have those
4 permissions.

5 If I may continue.

6 Q Yes.

7 A Having accessibility doesn't equate to
8 authorization. So a user wouldn't have the
9 authorization to do that executable. Or to load that
10 Wget. That would be a system and network
11 administrator.

12 Q Say that once -- having ability doesn't
13 equal authorization?

14 A Yes, ma'am. That's a fundamental principle
15 of 25-2.

16 Q In the training that you discussed in the
17 CDs, does that tell users that?

18 A Yes, ma'am.

19 Q So if a user goes on the internet or is,
20 sends an e-mail with some kind of an attached movie or
21 clip or something like that, is that considered an

1 executable file?

2 A Many times it can be, yes, ma'am.

3 Q So if the user clicks on the clip, is that
4 a violation of AR25-2?

5 A By policy, yes, ma'am. Because you have no
6 idea what the content of that movie file may contain.
7 It should be reported as a potential security violation
8 or an attempt by somebody to do malicious activity on
9 your network.

10 Q I guess that's back to my original
11 question. When machines, when users are on Army
12 machines normally if the user tries to install
13 something they're not allow to install, don't they get
14 the box that says they have to have the administrator
15 privileges?

16 A Yes, ma'am. Many times.

17 Q But not always?

18 A But based on how -- clicking on the link in
19 the e-mail may contain malicious content that might
20 load onto the computer but may not execute until the
21 next time you log off and log back on, for example. Or

1 other actions that circumvent the security parameters
2 of that system.

3 So the user would click on a link, the code
4 would execute, he would not see those pop-ups or may
5 not see those pop-ups. And then your system is
6 compromised. Not all actions are identified by the
7 system when you install or maliciously accessed content
8 that might be sent to you.

9 Q Assume there is mission related. Someone
10 sends a video or someone sends some kind of a file that
11 you open and execute. Is the user prohibited from
12 doing that?

13 A No, ma'am. But it's usually part of the
14 operational process by which the process itself, the
15 control mechanisms are in place and the process has
16 been validated to be either safe or approved. So
17 sending UA video from side A to B or moving a file from
18 side A to B that's a UAV video would be operation and
19 so, you know, double clicking on that executed is, is
20 approved or authorized.

21 THE COURT: Any questions based on mine?

1 MR. Von ELTEN: Nothing, Your Honor.

2 MR. TOOMAN: None.

3 THE COURT: Temporary or permanent excusal?

4 MR. Von ELTEN: Temporary.

5 THE COURT: You are temporarily excused.

6 Please don't discuss your testimony with anyone other
7 than the lawyers and the accused while the trial is
8 going on.

9 THE WITNESS: Absolutely, ma'am. Thank
10 you.

11 MR. FEIN: Your Honor, the United States
12 offers to read a stipulation into the record. This is
13 Prosecution Exhibit 80.

14 Stipulation of expected testimony for
15 Mr. Doug Schasteen dated 9 June 2013.

16 (Whereupon, Prosecution Exhibit 80,
17 stipulated testimony of Doug Schasteen, was read into
18 the record.)

19 MR. FEIN: United States moves to admit
20 Prosecution Exhibit 114 for identification as
21 Prosecution Exhibit 114.

1 THE COURT: Any objection?

2 MR. COOMBS: No objection, Your Honor.

3 THE COURT: Prosecution Exhibit 114 is
4 admitted.

5 MR. Von ELTEN: Ma'am, the United States
6 calls Mark Kitz to the stand.
7 Whereupon,

8 MARK KITZ,
9 called as a witness, having been first duly sworn to
10 tell the truth, the whole truth, and nothing but the
11 truth, was examined and testified as follows:

12 EXAMINATION BY MR. Von ELTEN:

13 Q Are you Mark Kitz of Aberdeen, Maryland?

14 A Yes.

15 Q Where do you work?

16 A I work at Aberdeen Proving Ground in
17 Maryland at the Program Executive Office Intelligence
18 Electronic Warfare Surveillance Program Manager
19 Distributed Common Ground System Army.

20 Q What is your educational background?

21 A I have a bachelor's degree from Lafayette

1 College in electrical engineering and a master's degree
2 in electrical engineering as well from New Jersey
3 Institute of Technology with a focus on communication
4 systems.

5 Q How long have you been a government
6 employee?

7 A About 13 years.

8 Q And what have you done in your time for the
9 government?

10 A So I came to the government directly out of
11 college. I have worked on my master's program while I
12 was in college, I mean, sorry, while I was employed by
13 the government.

14 I worked for the Trojan program, the
15 acronym totally escapes me. It's a communication
16 system. I was the project engineer, project leader,
17 project manager and I spent about six or seven years
18 with the Trojan program working on the communication
19 systems and then they also have an intelligence system
20 that I was a project manager on as well.

21 Then I did, I was selected for engineering

1 and scientist exchange rotation in Australia. I did a
2 year and a half at the Defense Science and Technology
3 Organization in Australia.

4 Then I came back and began working on D6-A
5 on a loan from a S and T community and then went as a
6 core employee or working directly for the program
7 manager in 2011.

8 Q How long have you worked at D6-A?

9 A It's a little over five years.

10 Q What position did you have prior to your
11 current one?

12 A I started as a integrated product team lead
13 for installs intelligence and then I worked my way up
14 to becoming the systems engineer lead for a product
15 that we have called Version 3 or the intelligence
16 fusion server and basic (INAUDIBLE) laptop.

17 Then I was selected to become the technical
18 director for the program which is the role I currently
19 have which oversees a portfolio of systems, capacity
20 abilities and software across the D6-A portfolio.

21 Q How large is that portfolio?

1 A So we're an ACAT 1 MAIS, an automated
2 information system. There isn't a larger category of
3 acquisition programs in the defense so we're a very
4 large program.

5 We have a portfolio of about 13 systems
6 fielded from company to (INAUDIBLE). We have over 700
7 server suites, over 5,000 laptops. We field to support
8 the full 58,000 military intelligence professionals
9 supporting the Army.

10 Q What is D6-A?

11 A So D6-A is essentially a portfolio of
12 capabilities providing intelligence, processing,
13 exploration and dissemination for the Army.

14 What does that mean in lay terms? Every
15 military intelligence analyst in the Army gets D6-A.
16 Whether that's a laptop, whether that's a server, back
17 end infrastructure for them to save data, store data,
18 whether that's a sensor flying over the battle space.
19 There's something on the ground ingesting that sensor
20 feed and providing that information to an analyst.

21 All of that infrastructure across the

1 entire Army is provided by D6-A.

2 It's relatively difficult to explain in
3 somewhat really lay terms but everything from the data
4 link itself, from the piece of satellite communications
5 that comes with it to the Microsoft Office product that
6 sits on a laptop is bought for by the D6-A program and
7 it is the acquisition program for that purchase or
8 procurement.

9 Q At what level are D6-A systems distributed?

10 A So today we're, all the way as low as the
11 company intelligence support team, so equipment to the
12 battalions and companies, D6-A headquarters, division
13 headquarters, at the core headquarters and then all the
14 support brigades and all of the above core elements
15 that have intelligence professionals are equipped with
16 D6-A.

17 Q Who do you advise in your current position?

18 A The program manager for D6-A, Cole Charles
19 Wells.

20 Q What does the program manager do?

21 A So the program manager is the chartered,

1 I'm struggling for the adjective, he is the person in
2 charge of all of the activities within the portfolio.
3 So the ACAT 1 program we mentioned called D6-A.

4 Also an ECAT 2 program and ECAT 3 program
5 called charts, counterintelligence, human intelligence
6 capability for the Army. He manages that portfolio, as
7 the acquisition manager, and he certainly follows 5002,
8 the 5002 law in procuring capability against the
9 validated requirement by the JROC, by the joint
10 community.

11 Q What matters do you advise the program
12 manager on?

13 A Technical and acquisition. So as the
14 technical director I advise the program manager on
15 trade analysis, determining how we meet requirements
16 and what software or what hardware or what capabilities
17 are purchased and how the teams are advised -- how the
18 teams are proposing those procurement activities. Then
19 I also advise him on the acquisition process. How we
20 move through the gates that are put up by OSD and by
21 Congress that we have to statutorily or regulatorily

1 meet in order to achieve the capability for the war
2 fighter.

3 Q What do you consider when giving advice to
4 the program manager?

5 A So a lot of it comes down to my experience.
6 A lot of it comes down to essentially developing
7 courses of action that allow him to make an informed
8 decision about not just the technology, not just the
9 acquisition process but what is best and makes the most
10 common sense to achieve the goals of the program and
11 the Army.

12 Q How long have you been in your current
13 position?

14 A Two years.

15 Q Let's talk about the development process.
16 How would you characterize it?

17 A So the develop process is, I wouldn't call
18 it set in stone but it is a tried and true process from
19 an acquisition perspective. It's termed the systems
20 engineering process, that's essentially it lays out the
21 outline of how the Army procures systems at a large

1 level as I mentioned as ACAT 1 program. So that
2 process is well defined and it's taught across the
3 Army.

4 Did I answer your question?

5 Q You did.

6 Let's talk a little bit about creative
7 software setup. About how many steps are involved?

8 A So in identifying a solution to a piece of
9 software to meet a requirement, there's multiple steps
10 involved. The first would be defining the requirement.

11 So the Army system would have a requirement
12 that's defined in what we call our capabilities
13 production document, CPD or capability description
14 document called the CDD. We in D6-A since we're a
15 large program, we actually have both. The CDD
16 essentially says we want you to build a D6-A and the
17 CPD gets to further detail.

18 So the first step of the process is
19 ensuring that we have a solid requirement set that says
20 will go build something that makes sense for the Army
21 and is measurable via a test.

1 The next step would be to build organizing
2 principles around that requirement so in our CPD we
3 have 20 attributes. So each attribute has hundreds of
4 requirements associated with it. So we organize it to
5 integrated product teams as I mentioned earlier. So
6 integrated product teams are empowered to identify
7 solutions and build out their own process on how they
8 would address that requirement with a capability.

9 Q Who are on the integrated product teams?

10 A So you would have subject matter experts,
11 user representation from trade, from the training and
12 doctrine command and systems engineers like myself.

13 Q How do they evaluate product?

14 A So essentially you would evaluate the
15 requirement and refine the requirement into measurable
16 sets.

17 So the example I used previously is, the
18 requirement may say to go build a word processor and
19 that word processor, another requirement in a word
20 processor may be to, we want to it support English and
21 Arabic and Chinese. And so the requirement would then

1 be essentially decomposed into smaller chunks,
2 measurable chunks. You can't measure a requirement
3 that says build a word processor.

4 You can't delineate between different word
5 processing pieces of software that would deliver that
6 capability.

7 So the IPT would agree upon a set of
8 measurable requirements and do trade analysis.

9 Q What is trade analysis?

10 A So trade analysis would be similar to
11 releasing a request for proposals.

12 Essentially the government is looking for
13 this set of requirements to -- a solution that would
14 meet this set of requirements and they would do the
15 technical evaluation and the cost evaluation against
16 those requirements and then propose a solution back to
17 the larger program and the systems engineering process
18 that says, an example, I'm in the signals intelligence
19 IPT. I would propose this solution to meet a certain
20 requirement and the wider systems engineering community
21 would accept that through a series of gates.

1 Q What happens after the solution is
2 proposed?

3 A So the solution would be proposed at a
4 preliminary design review to the program manager and
5 the product manager. They would either get a go or no
6 go decision at that point on their approach and how
7 they would address a solution.

8 And they would then identify a solution and
9 propose that back at a critical design review.

10 And at the critical design review the
11 program manager would make a decision about the
12 baseline itself and whether or not under cost schedule
13 and performance parameters we can execute the solution.

14 Q What points of this process are you
15 involved with?

16 A So I'm involved in all parts of the process
17 as an oversight function today. Through my career in
18 D6 I've been, as I mentioned, an IPT lead, an IPT
19 engineer and a lead systems engineer on a product. So
20 I've seen how the process works from all points of view
21 in terms of the process.

1 But today that's where I sit. Most of my
2 functions is engaging with the office of the Secretary
3 of Defense who also acts as an oversight role as an
4 ACAT 1 program so I act as their conduit into the
5 program so they can better understand the objectives
6 and where we're trying to go.

7 Q What happens after the program manager
8 makes a decision?

9 A Essentially contracts are let and the
10 solution is built. After it's integrated and built we
11 go to what I call code and unit test and then
12 development test. Where we would have Army test, an
13 evaluate command come in and evaluates the solution
14 that was built and then upon successful completion of
15 development tests we would go into an operational test.

16 Q What is an operational test?

17 A An operational test is essentially an
18 operational unit using the system, stressing the system
19 and validating it that the system is effective,
20 suitable and survivable. Does the system work.

21 Q Let's talk about baselines. What is a

1 baseline?

2 A So for us a baseline is essentially the
3 hardware and software that we field and train to an
4 Army unit for them to use whatever piece of portfolio
5 that may be. So as we come out of that test, we
6 provide that software or that hardware or both in those
7 cases to the unit through a fielding process where we
8 train them, they sign for the equipment and that
9 baseline is then used as essentially their weapon
10 system.

11 Q What is of the purpose of the baseline?

12 A So the purpose of the baseline is the
13 process from requirements the operational test has, the
14 Army has validated a risk profile, the function
15 survivability essentially and the suitability.

16 So does the system work, will it work for a
17 long period of time and is it sustainable by Army
18 metrics.

19 So the Army process has val -- I shouldn't
20 say the Army process -- the process has validated those
21 things and so the baseline defines and defines a risk

1 profile for the Army with regard to will that baseline
2 meet the war fighter's requirements and work for that
3 war fighter.

4 Q You just mentioned risk profile. What are
5 some of the risks the process tries to prevent or
6 mitigate?

7 A So throughout the entire process, risk is,
8 a lot of the program manager's job is managing risk.
9 Essentially there's technical schedule and cost risk
10 associated with building any solution for the Army.
11 So managing that risk in all three of those
12 facets is critical to how a program manager executes
13 their job. So it's not just about technical
14 performance it's about the cost and schedule associated
15 in delivering that solution.

16 Q What role does bandwidth play in
17 determining the system setup?

18 A So in terms of the system setup, is that
19 what you asked?

20 Q Yes.

21 A So I think in terms of the system setup, I

1 would think that the system is designed to be set up or
2 to initially be set up without bandwidth. To be a
3 fully severable system -- I shouldn't say that.

4 Most of the portfolio, I guess all of the
5 portfolio can be set up without any communications
6 backbone. However, the communications backbone enables
7 the analyst access to information that they essentially
8 require for their job.

9 So the system is enabled by the
10 bandwidth that's provided but in order to set it up,
11 it's not required.

12 Q In the deployed environment, how many
13 communities might be on the same bandwidth?

14 A I don't know the answer to that question.

15 Q What is the portfolio security?

16 A So for us portfolio security is back to the
17 systems that I mentioned. D6-A delivers a common
18 ground station, an intelligence fusion server, multiple
19 pieces of the portfolio. So we manage security as a
20 portfolio. Can we connect to the network, is this
21 survivable in terms of vulnerabilities, are we

1 resilient to vulnerabilities.

2 So as the program manager, you're managing
3 that profile, again that risk profile in terms of
4 security in the solutions that you're building.

5 Q Why is it important?

6 A So for us, for a program manager delivering
7 a software solution what's really important is that
8 those soldiers have the capacity abilities that they
9 need. In order to do that they have to be able to
10 connect to the networks that they need. So for us it's
11 critical that we meet the requirements of the networks
12 that we connect to.

13 D6-A connects to six different nest works
14 by requirement. Along with the networks comes six
15 different requirement sets for those networks. It's
16 critical for us to maintain a positive security profile
17 and I say positive in terms of meeting those
18 requirements so that they can connect to the network
19 and get to the information that they need and the
20 systems can remain on the network.

21 Q What does Cyber hard mean?

1 A Cyber hard is a relatively new term for
2 something that we have had to do since the installation
3 of D6-A, which is essentially back to the security
4 point that we had mentioned before. We have to harden
5 the systems in order to meet the requirements of the
6 network.

7 So that means the OS has to be hardened,
8 has to go through the security checklists and it has to
9 be replicated across 5,000 laptops, across 700 servers,
10 so it's not something that, you know, we can expect
11 every client users to go through. It needs to be out
12 of the box that way every time so each user is not
13 concerned about the security profile of their system.
14 That comes inherent to the system that we're providing.

15 Q Let's talk about Wget. What is Wget?

16 A So Wget is -- I have a cursory knowledge of
17 Wget. Wget scrapes web sites, essentially uses FTP and
18 pulls down that information and allows you to export it
19 to multiple formats.

20 Q What do you mean when you say it scrapes
21 web sites?

1 A It essentially pulls the information off of
2 the web server.

3 Q How does Wget get through the authorization
4 process?

5 A To my knowledge, Wget has never been
6 authorized on a D6-A system.

7 MR. Von ELTEN: One moment, Your Honor.
8 Nothing further.

9 THE COURT: Cross-examination?

10 CROSS-EXAMINATION BY MR. TOOMAN:

11 Q Good afternoon, Mr. Kitz.

12 A Sir, how are you?

13 Q Well, thank you.

14 Mr. Kitz, you spoke on direct about the
15 process through which a program will get vetted to
16 become part of the baseline?

17 A Yes.

18 Q You mentioned, you used the term a couple
19 times ACAT 1. What does that mean?

20 A So it's a acquisition category. So
21 essentially, I don't actually know who, if it's

1 Congress or Department of Defense who sets these
2 categories but based upon the funding threshold for the
3 four year program, specifically RDT and E, research and
4 development funding determines how big your program is.

5 Number one is the biggest. There are also
6 2 and 3, 3 being relatively small. Off the top of my
7 head I don't remember the threshold. It's different if
8 you're an NDAP, Naval Development Acquisition Program.
9 It's different. We're actually called a MAIS, Major
10 Automated Informations System. You're an IT system,
11 you're buying software and hardware for the DoD.

12 Q So if you needed an ACAT 1 system, means
13 that it's one of the biggest programs in the Army,
14 correct?

15 A It is.

16 Q And with that comes a lot of oversight?

17 A Roger, sir.

18 Q Because there's a lot of money?

19 A Yes, sir.

20 Q Now, you talked about the process through
21 which a software program will become part of the

1 baseline and it starts with the requirements document,
2 correct?

3 A Roger, sir.

4 Q So when you get a requirements document,
5 let's use an example, you might get a requirements
6 document that says we need a word processor?

7 A Yes, sir.

8 Q So now we're going to try and find a word
9 processor that fits our needs, right?

10 A Correct.

11 Q So the first thing that happens then is you
12 come up with A spec and B specs?

13 A Yes, sir.

14 Q What's an A specs?

15 A It's that functional decomposition of the
16 requirement. So as you mentioned, word processor, so
17 the CPD would say, the Army, the D6-A needs to have a
18 word processor. You can't build a system based upon
19 that. So you need things.

20 So to give to a developer tasks to give to
21 a developer to actually build a word processor, what

1 are the tasks or those measurable things. Like I
2 mentioned, languages, back space, support for, you
3 know, external development. Those types of things
4 would be in an A spec and B spec. So when a tester
5 went through it and said, does this meet the
6 requirement, that's something measurable that that
7 tester can say yes, it supports Chinese language, all
8 characters, so on and so forth.

9 Q Okay. So we're going to have sort of a big
10 picture requirement of we need a word processor and
11 then we're going to burrow down even further and say it
12 needs to do English, Arabic?

13 A Yes, sir.

14 Q And needs to be able to save and I need to
15 bold?

16 A Exactly.

17 Q Any number of requirements?

18 A Exactly right.

19 Q Okay. So then it's going to go into the
20 sort of development phase. It's going to go to
21 integrated product teams?

1 A Yes, sir.

2 Q And those teams, what are they going to do
3 with it?

4 A So essentially IPT create the A specs and B
5 specs and they understand the task and charter of what
6 they have to build and then they will begin the process
7 to identify material solutions that will meet those
8 requirements.

9 So a word processor in this example, all of
10 those requirements would get to one team and that team
11 would then begin the process of identifying a solution
12 whether, that may be a solution the Army already has.
13 It may be something that we need to contract out for a
14 new development or it may be needs something that's
15 commercially readily available and we can go to
16 industry to get it.

17 Q So the IPT may say we have got Microsoft
18 Word, we have got open source or open office and
19 they're going to look at all of those things and see
20 which one fits?

21 A That's right. They would measure against

1 the cost schedule and performance of that. So the best
2 performing word processor may not be available to us
3 because of a cost prohibit -- or because it wouldn't be
4 able to meet the schedule for all the features we need.

5 Q And then the IPT are going to propose
6 solutions. They're ultimately going to say, for
7 example, let's go, well, Microsoft Word?

8 A Correct. As an ACAT 1 program we have two
9 gates we have to meet. PER, preliminary design review
10 and critical design review. At the gates we would
11 validate the design or proposed solution.

12 Q So there are multiple IPTs, correct? So
13 we're going to have IPT that are looking at the
14 software requirement from a number of different angles,
15 correct?

16 A Yes, sir, yes.

17 Q So then after each of those IPTs comes up
18 with the recommendations, then we're going to another
19 phase where someone sits down and looks at it all and
20 tries to eliminate redundancy?

21 A No, I wouldn't call it a separate phase.

1 There is a systems engineering IPT that conducts and
2 orchestrates this. Again, it's quite a large program.

3 So you're right. There's anywhere between
4 12 and 16 IPTs at D6-A at any one time, depending upon
5 the focus of how we're building the software. I would
6 not call them discrete entities in the process.
7 They're one sort of systems engineering IPT
8 orchestrating the sub IPTs.

9 Q Okay.

10 A It's a constant sort of rolling feedback in
11 terms of redundancy in terms of identifying solutions
12 that would meet more than one IPT's requirement.

13 Q So after the IPT it's then going to go to
14 initial design review?

15 A Yes, sir.

16 Q And at initial design review there are
17 going to be trade studies?

18 A Yes, sir.

19 Q So you're going to have industry members or
20 other groups studying the market and they're going to
21 give their input?

1 A No. It would still be the government
2 that's studying the market. But that would be the
3 point with which we would engage with industry to see
4 what's available.

5 Q So there you would reach out and see what's
6 already available or see what it cost to create
7 something new?

8 A Right, right.

9 Q And out of that, you're going to get a
10 proposed design, correct?

11 A Yes, sir.

12 Q And then you're going to have, that's sort
13 of the first stage. You're going to have go, no go,
14 this is what we're going to do or --

15 A Typically in my experience at initial
16 design review ends with a lot of things to do. So, you
17 know, you didn't quite meet the market and design.
18 Here's all the things you've got to do before your
19 final design phase.

20 Q Once you hit that gate, once you get to go,
21 at that phase, then you're going to go to operational

1 testing, correct?

2 A We go through a development phase,
3 essentially got to build after you finish designing.
4 You've got to finish building it and then you go to
5 test phase.

6 Q And then again you're going to have to get
7 a go or no go at the testing phase?

8 A Correct.

9 Q And then once all of that stuff is done,
10 we're going to have a baseline, a software program that
11 is becoming part of the baseline or gets approved?

12 A Defines the baseline, yes.

13 Q And that's all, that's a lengthy process?

14 A Yes, sir.

15 Q And it's a lengthy process because this is
16 a big program with a lot of oversight?

17 A Sure.

18 Q Now, updates to D6-A, the software
19 baseline, those typically happen on a 18 to 24-month
20 cycle?

21 A Yes, sir. To the baseline itself, yes.

1 Q So it's possible for a user, a unit that
2 may be deployed, to be operating on a system that is
3 old?

4 A Absolutely.

5 Q So it's possible for, if a unit deploys
6 December 10th and the new system comes out on
7 January 10th, they're really working with a system
8 that's 18 do 24 months old?

9 A I think you would not find the case. Once
10 a new software baseline has been defined, the theater
11 usually is priority and most units in theater elect to
12 upgrade the software once it's available.

13 So you're right in that 18 to 24 months
14 there's an older software baseline, once there's a new
15 one available, you'll find, my experience is units want
16 that new software and they would request it and get it.

17 Q So it happens in the field?

18 A Yes, sir.

19 Q Now, there are other ways that software can
20 be added in the field, correct?

21 A Yes, sir.

1 Q One such way would be to put in, to go
2 through this whole process. That would be one way,
3 right?

4 A Yes, sir.

5 Q And another way would be to ask for,
6 basically ask for an update, correct, or ask for
7 approval to put something on?

8 A Yes, sir. You can -- so once a baseline
9 has been defined, we stand up a process called
10 Engineering Change Review Board, ECRB. ECRB
11 essentially manages that baseline. And the program
12 manager does that for the first year that the baseline
13 is defined and then we transition that to the
14 communications electronics command, also located at
15 Aberdeen Proving Ground. That manages the sustainment
16 of that system. So they're funded to ensure that the
17 baseline remains current, relevant and they manage that
18 process for the engineering review.

19 Q Now, it's possible that a unit may want to
20 add something to their system and not want to go
21 through any of those processes, correct?

1 A Absolutely.

2 Q And that unit may decided we're just going
3 to do it and not check with anyone?

4 A I imagine that that's possible. However
5 the unit is not authorized to change the baseline.
6 That's not something that -- there's no sort of process
7 for that, if you will.

8 Q Sure. The unit may say, I don't really
9 want to go through this long testing process. I don't
10 really, you know, we're deployed, we don't want to deal
11 with these hoops. We just want to get the mission
12 done. We're going to put it on there.

13 A Yes, they may do that. I, I'm not certain
14 how, what the process would be, but yes, they may do
15 that.

16 Q You spoke about Wget and you talked about
17 Wget being a secure FTP program?

18 A I'm not certain that it uses FTP. It's a
19 different protocol from FTP. I only have a personal
20 knowledge of Wget from these proceedings. But yes, I
21 did speak of it.

1 Q There are a lot of programming out there
2 that are safe that have never been approved part of the
3 baseline?

4 A That's true.

5 Q And that's because they've not been tested?

6 A Or they may not have a requirement to be on
7 the baseline.

8 Q Okay. Now, there is a secure FTP program,
9 it's part of the baseline, isn't it?

10 A Yes, sir.

11 Q And that is a program called Save Move?

12 A Yes, sir.

13 Q That program essentially has the same
14 abilities as Wget in that it can be used to go out and
15 download entire web pages if you wanted?

16 THE COURT: What's the name of the program?

17 MR. TOOMAN: Save Move.

18 A Save Move was designed to essentially pull
19 files. So can it take web pages? Yes, it would have
20 to access the web server and get to the files behind
21 it. It's a little bit of a different design but

1 absolutely. It is a FTP to move files and it is loaded
2 on the D6-A system.

3 Q Now, you spoke about connectivity and you
4 mentioned that the D6-A system is a system that does
5 not have to be connected but in reality if it's not
6 connected it's kind of worthless, right?

7 A I wouldn't use that term because you still
8 have all the commercial tools available to you that you
9 would need to do your job. But if you're not
10 connected, you know, obviously your data pool is very
11 small comparatively.

12 Q You need the connectivity to access
13 information from various databases?

14 A Yes, sir.

15 Q And that's the information that you're
16 going to use to create your work product?

17 A Yes, sir.

18 Q Now, Mr. Kitz, do you know whether or not
19 soldiers today are allowed to work on their D6-A
20 machine and by work on it, I mean modify it or tinker
21 with it?

1 A They are not authorized. We have a recent
2 program to allow soldiers that are authorized, but
3 there's a very small number of soldiers today
4 authorized admin., what I would term admin. rights to
5 the system.

6 Q So in the past, how it would work would be
7 you would have a deployed unit and they would have a
8 D6-A contractor that would be sort of embedded with the
9 unit?

10 A Yes, sir.

11 Q And that individual would be the one who
12 would work on the machines?

13 A Yes, sir, field service engineer.

14 Q And now today we have, in some cases,
15 soldiers are able to do the same functions?

16 A Only in one instance, yes, sir.

17 Q Now, when a unit deploys and they come back
18 to the states, D6-A, the machines get scrubs, don't
19 they?

20 A No, I don't -- I'm not -- ask your question
21 again. I don't believe I quite understood it.

1 Q Sorry. I'll rephrase. When a soldier
2 redeploys and come back to the states, what happens to
3 the D6-A machines?

4 A Totally up to the unit. The program does
5 nothing with the system. There's a program called
6 reset, blows the dust out of it and make sure
7 everything works and turns on. But from the programmer
8 perspective, we don't touch the software in the system.
9 The system remains the way it was when the unit comes
10 back with it.

11 Q And when a unit has their D6-A machines
12 updated, that would be something that is done by a
13 D6-A --

14 A Yes, sir.

15 Q And that person would look at what's on the
16 D6-A machine that they're updating, correct?

17 A No, I would not make that assumption
18 because when the program goes out to update a baseline,
19 they're providing a new baseline to that system. So
20 essentially they are actually reloading the entire
21 system and moving the data over.

1 So I'm not certain that they would, I would
2 use the term scrub the old system because I don't think
3 that they necessarily are concerned about the specifics
4 are what on that system. They're concerned about the
5 data that was there and updating that system. And in a
6 lot of cases, they would get a new physical system,
7 depending upon how old the hardware was.

8 Q If they got a new system, what would happen
9 to the old system?

10 A Actually the PM would take ownership of
11 that system and they would have disposition
12 instructions associated with it.

13 Q Sir, are you aware of whether or not it's
14 common for D6-A systems to have unauthorized software
15 or unauthorized files on them?

16 A I'm not in a position where I have direct
17 knowledge of that but it is my understanding that it is
18 relatively common, yes, sir.

19 MR. TOOMAN: Nothing further. Thank you,
20 Mr. Kitz.

21 REDIRECT EXAMINATION BY MR. Von ELTEN:

1 Q Who uses Save Move?

2 A The only people is the field service
3 engineer. They are the only people that have access to
4 that application.

5 Q What side does Save Move operate on?

6 A Entirely server side operation. So there's
7 no Save Move loaded on a client.

8 Q What side is a user on?

9 A Just the client side.

10 Q When is a user on the network side or
11 system side?

12 A The user does not have access to the system
13 as a client user. Only an admin. right would have
14 access to the operations on the server.

15 Q What side does Wget operate on?

16 A You can run it on the server or the client.

17 Q What side does Wget operate on if it's used
18 from an analyst laptop?

19 A It would be the client.

20 MR. Von ELTEN: Thank you.

21 THE COURT: I just have a couple of

1 questions for you.

2 EXAMINATION BY THE COURT:

3 Q Is mIRC chat on the list of authorized
4 programs?

5 A It is not on the list of authorized
6 programs, ma'am. There was a technical bulletin
7 released to our field service engineers that outlined
8 how to load it if a commander chose to load it. But it
9 is not on the official baseline and that letter that
10 went out the engineers essentially showed it because we
11 understood that a lot of commanders wanted mIRC chat.

12 So essentially that letter outlined that it
13 is not part of the baseline and any cost associated
14 with Microsoft Office as it is a licensed product as
15 well, was the commander's risk and the commander of
16 that unit had to procure it.

17 Q So let's go back to the commander's
18 authority again. If a commander is out in the field
19 and wants to install mIRC chat for example, do they
20 have to -- you said you sent a letter because you have
21 systems engineers that accompany the units that help

1 them with their D6-A computers?

2 A Yes.

3 Q So does the commander have to use that D6-A
4 engineer to load the program?

5 A Yes, ma'am. The engineer is the only
6 person that has the admin. rights to the system.

7 What I said, I should qualify that. We
8 have a process, it's called a technical bulletin. So
9 as, let's say a security update comes out for Oracle
10 and Oracle is on the system. We release a technical
11 bulletin. Here, field service engineer, this is how
12 you would apply this security patch to Oracle.

13 So we release the technical bulletin saying
14 that we understand that commanders have been requesting
15 this, it is not authorized, we, program manager, are
16 not authorized to allow you to have it.

17 However, we understand that the commander
18 wants to take the risk. If the commander sends us a
19 letter then we will allow it to be loaded.

20 Q So on a D6-A computer, if a individual user
21 wanted to load mIRC chat or Wget or any other type of

1 program and they tried to do it, would the computer
2 itself stop the user from doing that, with the little
3 box that says you don't have admin. rights?

4 A Yes, ma'am.

5 Q Would the same be true if the program was
6 on a shared drive?

7 A Yes, ma'am. Once it accessed essentially
8 the registry, it should kick and say, you require a
9 password to load any software on the system.

10 Q So the software program is on a shared
11 drive and the user reaches out on the shared drive and
12 takes it back on the local drive that message should
13 come up?

14 A Yes, ma'am. Once they tried to install it.

15 Q Could they put a shortcut from the shared
16 drive on their system?

17 A I don't believe so, no. The software has
18 to run from somewhere.

19 Q How about music games and that kind of
20 thing, can those be updated from a user to a D6-A
21 computer?

1 A (INAUDIBLE).

2 Q What's the difference between that and Wget
3 (INAUDIBLE)?

4 A Say there's a music player already on the
5 system. It really just uses the file system.

6 An example with Wget can be you can
7 download Wget or put Wget on the system, the file
8 itself. Once you try to run it, you would be required
9 admin. rights.

10 THE COURT: Any follow-up questions based
11 on mine?

12 MR. Von ELTEN: No, ma'am.

13 MR. TOOMAN: Just a couple, ma'am.

14 RECROSS EXAMINATION BY MR. TOOMAN:

15 Q You mentioned a memoranda that you sent out
16 to commanders because you understood that they wanted
17 to use mischaracterize chat. Does that recommendation
18 or guidance identify a particular version?

19 A Let me qualify your question. It wasn't
20 sent to commanders. It was sent to field service
21 engineers giving them guidance if the commander asks

1 you to install this. This is what's required of the
2 commander and this is how you would do it. I do not
3 know offhand, no.

4 THE COURT: Before you continue, let me ask
5 one more question.

6 When was that technical bulletin issued?

7 THE WITNESS: I believe it is in 2008,
8 ma'am.

9 THE COURT: Thank you.

10 BY MR. TOOMAN:

11 Q And a commander had to approve the addition
12 of the mIRC chat?

13 A Yes, the commander specifically had to
14 accept the risk.

15 Q Mr. Kitz, would it be possible to add mIRC
16 chat onto the desktop as an executable file?

17 A Without admin. rights?

18 Q Yes.

19 A I don't believe so.

20 Q What about Wget?

21 A I don't believe so.

1 MR. TOOMAN: Thank you, Mr. Kitz.

2 REDIRECT EXAMINATION BY MR. Von ELTEN:

3 Q Mr. Kitz, how do you install Wget?

4 A I've actually never installed it on my
5 machine so I would not be able to necessarily answer
6 that question.

7 Q How do you install mIRC chat?

8 A MIRC chat you have to download and it
9 probably has an MSI file that allows, that has
10 automated, you know, installation instructions and you
11 click through next like you would most applications.

12 Q How sure are you about mIRC chat?

13 A How sure am I with regard to what?

14 Q Its installation?

15 A How sure am I about what about its
16 installation?

17 Q The process.

18 THE COURT: I thought he just said he
19 didn't know how to install it.

20 Did I misunderstood your testimony?

21 A No, he asked me mIRC chat. And mIRC chat I

1 have installed before. So I'm relatively confident
2 that mIRC chat, you know, requires some sort of
3 interaction with the user to install it.

4 Q When you said MSCI --

5 A MSI.

6 Q What is an MSI?

7 A An MSI is essentially a wrapper around an
8 application that automates installation so whenever you
9 download a file on the internet and you bring up, I
10 want to double click and install it, it brings up a,
11 you know, who are you and then next here's the service
12 agreement between me and the user. Next is what are
13 the configurations, you know. I need an IP address for
14 the chat server Microsoft Office will connect to, then
15 you click next, yes. And the MSI file is essentially
16 the wrapper that allows the interface with the user to
17 configure and install the application.

18 MR. Von ELTEN: Thank you.

19 THE COURT: Temporary or permanent excusal?

20 MR. Von ELTEN: Temporarily.

21 THE COURT: Mr. Kitz, you're temporarily

1 excused. Please don't discuss your testimony or
2 knowledge about the case with anyone other than the
3 lawyers or accused while the trial is going on.

4 THE WITNESS: Sure. Thank you, ma'am.

5 MR. FEIN: The United States offers to read
6 a stipulation of expected testimony on the record.

7 THE COURT: Proceed.

8 MR. FEIN: This is Prosecution Exhibit 107.
9 Stipulation of the expected testimony of Ms. Florinda
10 White dated June 10, 2013.

11 (Whereupon, Prosecution Exhibit 107,
12 stipulated testimony of Florinda White, was read into
13 the record.)

14 THE PROSECUTION: The United States calls
15 Captain Thomas Cherepko.

16 MR. COOMBS: Could we a 10-minute break?

17 (Brief recess taken.)

18 THE COURT: Court is called to order. Let
19 the record reflect all attorneys present when the court
20 last recessed are again present in court.

21 Before we proceed I have been advised that

1 we now have a new piece of equipment in the court room.
2 Is that correct?

3 MR. FEIN: Well, ma'am, it's been moved
4 since then during recess, but yes.

5 THE COURT: Why don't we just go ahead and
6 put it on the witness stand and have someone sit in the
7 witness chair to see if there are any issues.

8 MR. FEIN: I'm placing a three-sided box to
9 block the witness.

10 THE COURT: Let the record reflect that the
11 court security officer is in the witness chair and we
12 are testing, it is a black covering that goes above
13 where the witness chair ends basically up to the
14 witness, a little lower than the witness' neck and that
15 is to ensure that classified information is protected.

16 SECURITY OFFICER: Test.

17 THE COURT: It appears the classified
18 information is protected. Any issues with the ability
19 to observe the witness?

20 MR. COOMBS: No, Your Honor.

21 THE COURT: Any other issues with the new

1 piece of equipment?

2 MR. FEIN: No, ma'am.

3 THE COURT: We can go ahead and move it
4 back then. Thank you.

5 Are you ready to call your next witness?

6 THE PROSECUTION: The United States calls
7 Thomas Cherepko.

8 WHEREUPON,

9 THOMAS CHEREPKO,
10 called as a witness, having been first duly sworn to
11 tell the truth, the whole truth, and nothing but the
12 truth, was examined and testified as follows:

13 DIRECT EXAMINATION BY MR. WHYTE:

14 Q You are Captain Tom Cherepko from
15 Pittsburgh, Pennsylvania?

16 A Yes, sir.

17 Q Captain Cherepko, what is your current
18 position?

19 A CIS plans and operation officer for NATO
20 Force Command Madrid.

21 Q What is CIS?

1 A Communications and information systems.

2 Q What are your responsibilities in this
3 position?

4 A I do planning for training exercises and
5 real world operations.

6 Q Captain Cherepko, what is your branch?

7 A I am a functional area 53 basic branch
8 engineer.

9 Q And what training did you receive to become
10 a 53 alpha?

11 A I went through the 53 alpha course long
12 known as the information system manager course.

13 Q Where was it?

14 A Ft. Worth, Georgia.

15 Q How long was it?

16 A Approximately nine months.

17 Q Can you please describe to the court what
18 this training consisted of?

19 A The course is broken down into three
20 phases, networking, enterprise systems with the
21 Microsoft Academy and third phase is security, other

1 related topics.

2 Q And what certificates did you receive
3 during this time?

4 A I received a CISSP, the Certified
5 Information Systems Security Professional, security
6 plus and the Windows Vista certification.

7 Q What was your first assignment out of this
8 court?

9 A 2nd Brigade, 210th Mountain.

10 Q When did you arrive at Ft. Drum?

11 A October 1st, 2009.

12 Q And what happened when you arrived?

13 A When I arrived, after I didn't process, the
14 brigade was in the process of deploying and within a
15 few weeks of my arrival I deployed with the brigade.

16 Q Where did you deploy to?

17 A To FOB Hammer, Iraq.

18 Q When did you arrive at FOB Hammer?

19 A Middle of November, sometime after the
20 relief in place with the 2nd Airborne.

21 Q Did PFC Manning deploy to FOB Hammer as

1 well?

2 A Yes, sir.

3 Q What section were a signed to at FOB
4 Hammer?

5 A The S6 communication section.

6 Q What was your position at FOB Hammer?

7 A I was the brigade automations officer.

8 Q What were your responsibilities in that
9 position?

10 A My responsibilities were the maintenance
11 and managements of the brigade's network in the absence
12 of the brigade signal officer, act as the brigade
13 signal officer and information assurance manager.

14 Q So you said you were responsible for the
15 maintenance of the network?

16 A Yes, sir.

17 Q What classified networks were available at
18 FOB Hammer?

19 A We had SIPRNET.

20 Q What was required for someone to get access
21 to SIPRNET?

1 A In order to get access for SIPRNET they
2 needed to have forms that were filled out that were
3 signed by the first line supervisor stating that they
4 had a need to have access to the network. The S2
5 section was signed verifying the security clearance and
6 then they would take the form to the help desk where
7 the account was created, assuming that their IA
8 training was complete.

9 Q So this was for them in order to get an
10 account?

11 A Yes, sir.

12 Q So what type of documents did they have to
13 fill out in order to get --

14 A They had to fill out the account request
15 for and an acceptable use policy.

16 Q And what type of training did they need to
17 receive in order to get a SIPRNET other?

18 A They needed to have the annual information
19 assurance training complete.

20 Q Was there exception to the IA training
21 requirement?

1 A No.

2 Q Was there exception to the AUP policy?

3 A No, sir.

4 Q What is a AUP?

5 A Acceptable use policy. It is a document
6 that states what you are and are not permitted to do on
7 the network that you are signing for.

8 Q What regulations are covered under AUP?

9 A AR25-2 and a few others.

10 Q Did PFC Manning have a SIPRNET other?

11 A Yes, sir.

12 Q How do you know that?

13 A Because on the night he was defiled I
14 deactivated his SIPR account.

15 Q And did he need to sign an AUP to get a
16 SIPRNET account?

17 A Yes, sir, everyone was required to.

18 Q Talk about the AUP. How many AUPs have you
19 signed in the course of your career?

20 A Approaching 50, sir.

21 Q When you arrived at Ft. Drum did you have

1 to sign an AUP?

2 A I did.

3 Q When you arrived at FOB Hammer did you have
4 to sign an AUP?

5 A Yes, sir.

6 Q Did all soldiers upon arrival at FOB Hammer
7 have to sign an AUP?

8 A All soldiers given accounts had to sign an
9 AUP, yes, sir.

10 Q And you said PFC Manning had an account?

11 A Yes, sir.

12 Q During the course of this investigation did
13 you locate PFC Manning's AUP?

14 A I did not, sir.

15 Q Was this the only AUP that you could not
16 find?

17 A No, sir. We were unable to find mine as
18 well.

19 Q Are you familiar with the contents of an
20 AUP?

21 A I am, yes, sir.

1 Q And what guidance is available for what
2 should be included in an AUP?

3 A AR25-2 has a sample AUP that we would use
4 to create an AUP.

5 Q Are you familiar with the sample?

6 A I am. Yes, sir.

7 Q How so?

8 A Upon redeployment I used the sample AUP to
9 draft the new AUP for the brigade with some other AUPs
10 as guidelines.

11 Q When you deployed back?

12 A When I redeployed from Iraq.

13 Q When you arrived at FOB Hammer did you
14 (INAUDIBLE) the AUP?

15 A I did, sir.

16 Q Can you explain how the sample AUP in the
17 AR25-2 compares to the actual AUP you signed at FOB
18 Hammer?

19 A They're similar sir. They may not look the
20 same but the content is similar.

21 Q So do you remember the AUP that you signed

1 at Hammer verbatim to the AUP in AR25-2?

2 A Most likely not.

3 Q Was the content of the AUP substantially
4 similar to the content?

5 A It would be similar.

6 Q Would you be able to identify the sample
7 AUP?

8 A I would, sir.

9 Q How would you be able to identify it?

10 A The sample AUP has generic terms throughout
11 that are meant to replace when you create your own
12 using it as a boilerplate template. For example, one
13 of them would be it doesn't have the name of the
14 network but it has classified network name and then the
15 acronym is CNN and I found it amusing that CNN is a
16 classified network so yes.

17 Q What other characterization about the
18 document?

19 A It says that it's a sample AUP and it has
20 several regulations, rules from AR25-2 listed in it.

21 Q Let the record reflect I'm retrieving

1 Prosecution Exhibit 94?

2 A It also starts on page 61, if that matters.

3 MR. COOMBS: Your Honor, the defense
4 objects to use of Prosecution Exhibit 49 for
5 identification. If I could, I believe trial counsel
6 brought out most of the foundation. If I can voir dire
7 in light of my objection for the matter of two or three
8 questions to show this is not relevant.

9 THE COURT: All right. Voir dire.

10 VOIR DIRE EXAMINATION BY MR. COOMBS:

11 Q You indicated that everyone signed an AUP
12 before they were given SIPRNET access in Iraq, correct?

13 A Yes, sir.

14 Q Was this the AUP everyone signed?

15 A That is a sample, sir, that is used as a
16 baseline to build the AUP.

17 Q So the answer would be no, this is not the
18 AUP that everyone signed?

19 A No, sir, this is not the actual AUP. It's
20 only a sample used to create an actual AUP.

21 Q And there is an actual AUP that had terms

1 that governed how an individual could use the SIPRNET?

2 A Yes, sir.

3 Q And everyone signed that?

4 A Yes, sir.

5 Q You said you couldn't locate PFC Manning's
6 and you couldn't locate yours?

7 A Correct, sir.

8 Q But you could locate other people's?

9 A Yes, sir.

10 MR. COMBS: So we would object to the use
11 of this sample AUP because this was not what was
12 signed. The government should be able to produce the
13 AUP that was signed by the soldiers from 210 Mountain
14 in order to get on the SIPRNET.

15 THE COURT: Captain Whyte, is there the
16 actual AUP that was signed?

17 MR. WHYTE: It couldn't be found. But the
18 sample AUP contained substantially all the content from
19 the AUP from his memory.

20 THE COURT: So this is a best evidence
21 objection.

1 MR. COOMBS: Yes, Your Honor, especially
2 when you have three specifications that rise and fall
3 on the (INAUDIBLE) so you've got specifications 2 and 3
4 of charge 3 and then each of those obviously are
5 (INAUDIBLE) violations and then you've got a 10-year
6 offense, specification 11 of charge II, a 10-year
7 offense.

8 If the government is going to premise
9 criminal liability based upon an AUP, they ought to be
10 able to produce the AUP. I understand maybe they can't
11 produce PFC Manning's. But we're talking about a whole
12 brigade. Surely at least one AUP can be found from the
13 brigade.

14 THE COURT: Government, normally I would
15 not, the government's allowed to try the case as you
16 want to, but in this, the government doesn't intend to
17 actually question about the actual document signed when
18 you have it.

19 MR. WHYTE: We intend to elicit testimony
20 from the witness about what was included in that AUP to
21 his memory, Your Honor, and the sample AUP will help

1 the witness testify to those things.

2 THE COURT: So would the AUP from Ft. Drum,
3 right?

4 MR. FEIN: Can we have a moment, Your
5 Honor?

6 THE COURT: Yes.

7 MR. WHYTE: Can I ask the witness a few
8 questions, Your Honor.

9 THE COURT: Yes.

10 DIRECT EXAMINATION BY MR. WHYTE:

11 Q Who maintained these AUPs at FOB Hammer?

12 A The help desk.

13 Q Originally what happened to these records
14 when they were signed?

15 A Yes, sir, they were collected from the
16 individual and then they were stored in a folder in the
17 help desk in the brigade headquarters.

18 Q Originally what happened to these records
19 once they were stored?

20 A They were stored just on a shelf in the
21 help desk area and they were --

1 Q Brief Your Honor with what happens to these
2 documents throughout their deployment.

3 A Yes, they remain just sitting in a folder.
4 They're never really referenced again unless we need
5 to.

6 Q Are you familiar with what happens once
7 you're redeployed?

8 A Yes, sir. Usually they're destroyed.

9 THE COURT: So there is no -- now I'm
10 completely confused. Is there or are there available
11 documents from FOB Hammer, AUPs that were signed by
12 somebody else or were not?

13 MR. FEIN: Ma'am, if I may?

14 BY MR. FEIN:

15 Q Captain Cherepko, do any AUPs from FOB
16 Hammer exist today?

17 A Not that I know of today.

18 Q Did they exist once you arrived back to Ft.
19 Drum?

20 A I don't recall any arriving back to Ft.
21 Drum, sir.

1 Q Because to the best of your memory what
2 happens to those AUPs that were in FOB Hammer in Iraq?

3 A When the network was turned off, they were
4 burned.

5 MR. FEIN: Thank you.

6 And there are no AUPs from Ft. Drum, excuse
7 me, from FOB Hammer when the unit redeployed because
8 they were destroyed which is why the United States is
9 offering to the best of his memory to be able to use a
10 sample AUP and to be able to draw, to aid him in his
11 memory what was on the AUP when it existed.

12 THE COURT: Do you want to voir dire the
13 witness further?

14 MR. COOMBS: Yes, Your Honor.

15 VOIR DIRE EXAMINATION BY MR. COOMBS:

16 Q Captain Cherepko, you said you eliminated
17 my client's ability to get on SIPRNET at some point?

18 A Yes, sir.

19 Q When was that?

20 A The night that he was detained.

21 Q So roughly towards the end of May 2010?

1 A I don't recall the exact date but yes, sir.

2 Q Prior to your redeployment?

3 A Yes, sir.

4 Q And at that point AUPs still existed,

5 right?

6 A Yes, sir.

7 Q But you hadn't redeployed?

8 A Correct.

9 Q So if the AUP wasn't secured at that point,
10 that was, that was because no one I guess asked for it?

11 A Or it didn't exist, yes, sir.

12 Q But somebody did come around looking for it
13 from you, correct?

14 A Yes, sir.

15 Q And they asked if you could produce it?

16 A Yes, sir.

17 Q And you said I can't find PFC Manning's?

18 A Correct.

19 Q But I can't even find mine?

20 A Correct.

21 Q But you had evidence at that point?

1 A In FOB Hammer, yes.

2 Q But no one asked for that dope?

3 A Not that I recall, no, sir.

4 Q And the government is attempting now to use
5 AR25-2 -- I'd like to have this marked as Defense
6 Exhibit Alpha for identification.

7 You said you used AR25-2 to create your own
8 AUP at some point?

9 A Upon redeployment, yes, sir.

10 Q And when you used your own, you added in
11 your own terms and whatnot?

12 A I did, sir. I used the sample from AR25-2,
13 the divisions and the installations and I made sure
14 that mine met the requirements of AR25-2 and was nested
15 with the divisions and the installations.

16 Q So was yours quite a bit longer than the
17 sample one in AR25-2?

18 A Yes, sir.

19 Q Was it worded verbatim to the one in
20 AR25-2?

21 A No, sir. There were sections that were

1 verbatim, but the complete document was not verbatim.
2 Because there are sections in the sample that you have
3 to modify to suit your unit and your local policies and
4 regulations.

5 Q I'm going to show you Defense Exhibit Alpha
6 for identification and see if you recognize it.

7 MR. FEIN: Ma'am, is this a voir dire?

8 THE COURT: I'm allowing it to see what
9 we're going to use.

10 Go ahead.

11 Q Showing you what's been marked as Defense
12 Exhibit Alpha for identification. Can you tell me what
13 it is?

14 A That is the Ft. Drum installation AUP.

15 Q What year and month is that AUP?

16 A February 2010.

17 Q So that would have been after your
18 deployment?

19 A It would have been in the middle of the
20 deployment, yes, sir.

21 Q As far as this one is for Ft. Drum,

1 correct?

2 A This is for the installation, yes, sir.

3 Q That wouldn't be the one that you would use
4 down (INAUDIBLE) would it?

5 A No, sir.

6 Q How many pages is that AUP?

7 A Seven, sir.

8 MR. COMBS: Retrieving Exhibit Alpha for
9 identification from the witness.

10 Your Honor, what the defense would ask the
11 court to do is look at Defense Exhibit Alpha for
12 identification and the version that the government
13 wants to use from 25-2 and you will see that there's
14 quite a bit of difference between the two versions,
15 this is what Ft. Drum used for AUP when they came back.

16 So if the government is going to premise
17 three specifications on a violation on 25-2 and one
18 (INAUDIBLE), violating the AUP for the 1030 offense,
19 the terms matter. It can't be closed.

20 I'm handing Defense Exhibit Alpha to the
21 court and I request that the court compare that with

1 Prosecution Exhibit 94 for identification.

2 THE COURT: I've looked at both of them,
3 Mr. Coombs. That's what they have cross-examination
4 for. You'll be free to question the witness about the
5 Ft. Drum AUP.

6 I'm going to let the government go ahead
7 and use Prosecution Exhibit 94 for identification. I
8 understand your objection.

9 MR. COOMBS: Ma'am, for clarification, it's
10 being used for illustrative purposes only. It's not
11 being used as the AUP signed by my client.

12 THE COURT: Yes. I believe that's the
13 government's position. Right? That's not the AUP
14 signed --

15 MR. WHYTE: That's correct, sir.

16 DIRECT EXAMINATION BY MR. WHYTE:

17 Q Handing the witness Prosecution Exhibit 94
18 for ID.

19 Captain Cherepko, please look at that
20 document and let me know when you're finished.

21 (Witness reading.)

1 A Yes, sir.

2 Q Are you familiar with this document?

3 A I am, sir.

4 Q What is that document?

5 A That is the sample acceptable use policy in
6 the back AR25-2.

7 Q And how do you know that?

8 A Because it starts on page 61 of AR-25. It
9 labels itself as the sample of acceptable use policy
10 and in the contents of it it uses the terms that are
11 being replaced with your specific unit information such
12 as classified network name, insert unit name here.
13 That sort of information.

14 Q Again, can you please explain to the court
15 how this sample, to the best of your memory, compares
16 with the actual AUP that you signed at FOB Hammer?

17 A It's similar. It may not look identical,
18 but the content is similar.

19 MR. WHYTE: Your Honor, we offer
20 Prosecution Exhibit 94 as the next Prosecution exhibit.

21 MR. COOMBS: Your Honor, the defense would

1 not and in this instance, I don't know if the witness
2 actually read the amount of time, this seems to be
3 similar meaning it looks like an AUP and there might be
4 some similar terms, but to offer this into actual
5 evidence in this case it has no relevance to this case
6 here because it's not what my client signed for one.

7 Second, even though the witness does have
8 personal knowledge of the AUP that was signed in this
9 instance all it's saying it's similar, most of the time
10 it might go to weight instead of admissible.

11 But in this instance because of the fact
12 that the terms actually matter, what is relevant is the
13 actual terms of AUP. So we would argue under 403 this
14 is also prejudicial and it is confusion of the actual
15 issues, that is what are the terms that PFC Manning had
16 to abide by while he was deployed.

17 THE COURT: Government?

18 MR. WHYTE: Well, Your Honor, actually the
19 Defense's exhibit as well was not a record that PFC
20 Manning actually saw himself. It was a document
21 produced or created during the deployment and signed

1 that document when he redeployed back at Drum which the
2 accused did not do. So that is not a document that PFC
3 Manning actually saw.

4 What we're asking Captain Cherepko to do is
5 based on this sample to testify as to what that AUP
6 that he signed at FOB Hammer consisted of.

7 THE COURT: Here's what I'm going to do
8 with that. With the foundation you laid so far, I'm
9 going to sustain the defense objection. If you want to
10 go through the document paragraph by paragraph and talk
11 about the witness, since he's coming from memory what
12 he remembers the actual AUP said, I'll listen.

13 MR. WHYTE: Just to clarify, Your Honor, we
14 can talk to the witness about what was included in the
15 FOB Hammer?

16 THE COURT: Yes.

17 MR. WHYTE: But not through reference of
18 Prosecution Exhibit 49 for ID.

19 THE COURT: You can use Prosecution Exhibit
20 94 for identification to go through the witness, this
21 is what the sample says, paragraph one. Was yours any

1 different. It the same. Was it --

2 MR. FEIN: May we have a brief moment?

3 THE COURT: Yes.

4 MR. WHYTE: Your Honor, we offer

5 Prosecution Exhibit 94 for ID as Prosecution Exhibit
6 94.

7 MR. COOMBS: Same objection.

8 THE COURT: After you've gone through the
9 paragraphs we'll address that.

10 May we have a short recess?

11 THE COURT: Yes, how long would you like?

12 MR. FEIN: Two minutes.

13 THE COURT: Captain Cherepko, please don't
14 discuss your knowledge of the case with anyone during
15 recess.

16 (Brief recess.)

17 THE COURT: Court is called to order.

18 Record reflect all parties present when the court last
19 recessed are again present in court.

20 Captain Whyte, witness is on the witness
21 chair.

1 MR. WHYTE: Permission to publish the
2 exhibit.

3 THE COURT: Proceed.

4 MR. WHYTE: I'm retrieving Prosecution
5 Exhibit 94 for ID from the court reporter.

6 BY MR. WHYTE:

7 Q Captain Cherepko, earlier you said that the
8 FOB Hammer AUP was nested from the sample AUP in
9 AR25-2. What do you mean by that?

10 A The one that I created after redeployment I
11 used AR25-2 sample as the baseline and I took my higher
12 head words and installations and make sure any local
13 policies that were in place were covered under my AUP.

14 MR. COOMBS: Your Honor, I object to
15 relevance of anything after the redeployment.

16 THE COURT: I believe the government's
17 question was the AUP, the AUPs that you used for Hammer
18 that you no longer, FOB Hammer, that you no longer
19 have.

20 THE WITNESS: Yes, ma'am. I didn't draft
21 that AUP. It was in place when I arrived at the FOB.

1 The only AUP that you crated was after redeployment.

2 THE COURT: Maybe you can target your
3 questions a little bit better.

4 BY MR. WHYTE:

5 Q Can you explain again how the sample AUP in
6 25-2 compared to the actual AUP that you signed at FOB
7 Hammer to the best of your memory?

8 A To the best of my memory the content was
9 very similar. The sample until 25-2 covers what needs
10 to be in an acceptable use policy and to the best of my
11 memory the content and the subject matter is very
12 similar.

13 Q Captain Cherepko, can you please just read
14 to yourself paragraph number one of Prosecution Exhibit
15 94 for ID.

16 (Witness reading.)

17 A Yes, sir.

18 Q So to the best of your memory, how did the
19 AUP that you signed at FOB Hammer compare to this
20 paragraph in the sample AUP?

21 A It may not have been verbatim, but it was

1 the same intent.

2 Q What was that intent?

3 A You're signing that you understand that the
4 2nd Brigade 10th Mountain SIPRNET or NIPRNET is, it's
5 your responsibility to follow the rules and not make
6 any unauthorized modifications, changes or do anything
7 to circumvent security.

8 Q Captain Cherepko, can you please read to
9 yourself paragraph 6.

10 (Witness reading.)

11 Q To the best of your memory, how did the AUP
12 that you signed at FOB Hammer compare to this sample
13 AUP in 25-2?

14 A Again, I can't recall verbatim what it
15 said, but the restriction on introducing software to
16 the network or to a system is prohibited, was
17 prohibited.

18 Q Are you familiar with what an executable
19 file is?

20 A Yes, sir.

21 Q What is an executable file?

1 A An executable file is a piece of software
2 that is able to be run without administrative
3 privileges. It wasn't required being installed, it
4 doesn't require any modifications of the operating
5 system and it can be run from a CD, a flash drive, from
6 a shared drive from a network location, from the
7 desktop. There's no, there's no requirement to install
8 an executable file.

9 Q When PFC Manning was at FOB Hammer, were
10 you familiar with what Wget was?

11 A When he was at FOB Hammer, no, sir.

12 Q But you're familiar with it today?

13 A Yes, sir.

14 Q What is Wget?

15 A It's an executable file that's used to
16 scrape sites or sources and retrieve any data that's
17 set in the parameters of the program to retrieve,
18 whether it's all or a specific type or what have you.

19 Q And to the best of your knowledge at FOB
20 Hammer was Wget an authorized executable file?

21 A It was not, no, sir.

1 Q Are you familiar with the certificate of
2 net worthiness?

3 A I am, sir.

4 Q What is the certificate of net worthiness?

5 A The certificate of net worthiness is an
6 organization for a piece of software to be used on Army
7 network.

8 Q When you were on the FOB Hammer was Wget on
9 this certificate of net worthiness?

10 A No, sir.

11 Q What does that mean?

12 A It was not authorized.

13 Q Captain Cherepko, if you could please read
14 subparagraph O.

15 (Witness reading.)

16 A Yes, sir.

17 Q To the best of your knowledge, how did the
18 AUP that you signed at FOB Hammer compare to
19 subparagraph O of the sample AUP?

20 A It would be very similar. That is a
21 required statement, not only on AUPs but every time you

1 log in the machine, that statement or one very similar
2 to it is displayed.

3 MR. WHYTE: Let the record reflect I'm
4 returning to the clerk Prosecution Exhibit 94 for ID.

5 BY MR. WHYTE:

6 Q Captain Cherepko, are you familiar with the
7 T-drive at FOB Hammer?

8 A I am.

9 Q What was the T-drive?

10 A The T-drive was a shared drive on the
11 network that users had access to to store files on.

12 Q And when you arrived at FOB Hammer, what
13 was the status of the T-drive?

14 A It was in place and operational.

15 Q And what network was it on?

16 A It was on SIPR.

17 Q What restrictions were placed on the
18 T-drive for access?

19 A If you were not a member of the 2nd Brigade
20 10th Mountain domain, you did not have access to the
21 shared drive. And if you were a member of the domain,

1 there were very few restrictions on where you could
2 view, edit or remove files.

3 Q So what prevented a user from moving
4 information on the T-drive?

5 A Nothing, sir. The intent of the T-drive is
6 to place information there, retrieve information so
7 that you don't fill up the local storage on your
8 computer.

9 Q And what prevented the users from removing
10 something from the T-drive?

11 A Nothing, sir.

12 Q Let's talk about the administrative rights
13 with the network. Who is an administrator?

14 A An administrator is a person with elevated
15 privileges that allows him or her to make modifications
16 to software or hardware.

17 Q So what is, just explain again, what does
18 it mean to have administrative rights?

19 A It means you have the ability to install
20 hardware, make changes to the operating system or
21 install software.

1 Q So what can a user not do without being the
2 administrator?

3 A They cannot install hardware and they
4 cannot install software. They cannot make
5 modifications or changes to the operating system.

6 Q What were the administrators of the share
7 drive?

8 A The administrators of the shared drive were
9 my soldiers and assistant administrators who worked for
10 me.

11 Q Did PFC Manning have administrative
12 privileges?

13 A No.

14 Q Was PFC Manning authorized to install
15 software?

16 A No, sir.

17 Q What happens if someone wanted to install
18 software onto their government computer?

19 A They would request a piece of software that
20 they did not have through the help desk and then the
21 help desk would check, if it was an authorized piece of

1 software that we had a license for and readily
2 available, they will install it. If it was not either
3 available or we did not have a license or it was not
4 authorized, then the help desk would come see me.

5 Q What would you do?

6 A I would then research the availability of
7 obtaining the software.

8 Q Would you check to see if an approved
9 program?

10 A I would, yes, sir.

11 Q At FOB Hammer to the best of your memory,
12 did PFC Manning ever ask you to install a program onto
13 his computer?

14 A No, sir.

15 Q You testified earlier that you are familiar
16 with Wget. Can you just one last time explain the
17 installation process for Wget?

18 A There is no installation process. If you
19 have it on a CD or thumb drive or on your desktop you
20 can simply run it. There's no administrative rights
21 required.

1 Q You said Wget was an executable file?

2 A Yes.

3 Q So how does using an executable file like
4 Wget allow a user to circumvent the need to actually
5 come see the S6?

6 A There's no administrator required to
7 install it. You simply run it from a disk or desktop.

8 Q So who was capable of putting a program
9 like Wget, an executable file, onto their computer?

10 A Anyone.

11 Q Was PFC Manning authorized to put Wget onto
12 his computer?

13 A No, sir. No one was.

14 Q What Army regulation prohibits soldiers
15 from using unauthorized executable files?

16 A AR25-2.

17 Q And what document do soldiers sign that
18 prohibits them from using unauthorized executable
19 files?

20 A An acceptable use policy.

21 Q What type of software is Wget?

1 A I believe it's freeware.

2 Q And what is freeware?

3 A Freeware is software that you can download
4 from the internet or whatever source you obtain it from
5 and you do not have to pay for it.

6 Q Is freeware authorized?

7 A It is not. It is specifically prohibited.

8 Q Under what?

9 A AR25-2.

10 MR. WHYTE: One moment, Your Honor.

11 BY MR. WHYTE:

12 Q So you testified earlier that you were the
13 administrator. You were one of the administrators?

14 A I was; yes, sir.

15 Q What were you the administrator of?

16 A I was the manager of all of the
17 administrators and by necessity I was also the senior
18 administrator for the brigade. Any problems that the
19 help desk soldiers or any of my technicians couldn't
20 solve, they would bring to me for the network, LAN,
21 WAN, enterprise services, local desktop computers, VTC

1 suites, battlefield command systems, any of the command
2 control systems.

3 Q Are you familiar with D6 machines?

4 A Slightly familiar, yes, sir.

5 Q Did you have D6 machines at --

6 A I believe we did, yes, sir.

7 Q Were you the administrator of the D6?

8 A I was not.

9 Q Who was the administrator?

10 A I'm not sure.

11 MR. WHYTE: No more questions, Your Honor.

12 CROSS-EXAMINATION BY MR. COOMBS:

13 Q Captain Cherepko, just for a moment to talk
14 about the AUP that you were shown. You talk about
15 something being, I think it might be similar, am I
16 correct that you read this once when you got to FOB
17 Hammer and signed it?

18 A The 2nd brigade AUP?

19 Q Right.

20 A Yes, sir.

21 Q And after that you weren't reading it on a

1 daily basis, were you?

2 A No, sir, not on a daily basis.

3 Q Were you in charge of briefing other people
4 on the AUP and having them sign it and supervise them
5 signing it?

6 A No, sir. I delegated that to my help desk
7 NCIC.

8 Q So you weren't even reviewing the AUP on a
9 daily basis?

10 A No, sir.

11 Q So when you talked about it looked similar,
12 you're basing that on a memory of seeing the document,
13 the one that was signed by you when you deployed in
14 2009, right?

15 A Yes, sir.

16 Q And now in 2013, that's where you're
17 testifying based upon that memory, back in 2009; is
18 that right?

19 A Yes, sir.

20 Q And when you say I think that's, you know,
21 similar or I believe that was in there, do you know

1 that or are you making basically an educated guess
2 based upon what you would think would be in there?

3 A I'm making a logical assumption that when
4 you create an AUP the best business practice is to take
5 the example that the Army gives you and says this is
6 the standard and you use that, along with local
7 policies and you create your document and every AUP
8 I've ever seen has very similar content.

9 Q Okay. I showed you Defense Exhibit Alpha
10 for identification and you agree with me that is much
11 more substantial than what is, what was shown for, to
12 you from 25-2, correct?

13 A Yes, sir. But the actual content and
14 quantity of content will vary from location to location
15 and within a local installation because most of that is
16 local policies that is added by the command creating
17 the AUP.

18 Q All right. Now, even within the AUP, the
19 one term that the government had you look at with, you
20 know, I will not add malicious code or whatnot, had a
21 phrase in there without authorization, correct?

1 A I believe so, sir. I don't recall what it
2 said but yes.

3 Q You don't recall something you just read a
4 few minutes ago?

5 A Yes, sir.

6 Q Okay. So do you need me to refresh your
7 memory on something you read a few minutes ago?

8 A No, I'm fine. We're good.

9 Q So, again, did it say without authorization
10 in it?

11 A On the sample AUP, sir?

12 Q Correct.

13 A I would, if you could refresh me that would
14 be great.

15 Q I'll be glad to.

16 Can I retrieve --

17 THE COURT: Are you referring to
18 Prosecution Exhibit 94 or Defense Exhibit Alpha?

19 Q Prosecution Exhibit 94 ma'am.

20 This is something that the government went
21 over with you a few minutes ago and they asked you to

1 read it to yourself?

2 A Yes, sir, I see it.

3 Q And you read that and they asked you, you
4 know, is this the one that you signed. You said I
5 believe so.

6 So now just refreshing your memory, do you
7 see without authorization?

8 A I do. Yes, sir.

9 Q So that would mean that if you obtain
10 authorization you could do it, I imagine?

11 A Yes, sir.

12 MR. COOMBS: Returning Prosecution Exhibit
13 94 to the court reporter.

14 BY MR. COOMBS:

15 Q Now, you said you were the brigade's
16 automation officer for the 2nd BCT?

17 A Yes, sir.

18 Q Your primary duty as I understood it was to
19 manage, maintain and secure the brigade's digital
20 communications; is that right?

21 A Yes, sir.

1 Q And as the brigade automations officer, you
2 were also the information assurance manager for the
3 brigade, the IAM?

4 A Yes, sir.

5 Q You were appointed to this duty on orders?

6 A I was, sir.

7 Q And as the IM you were the person in charge
8 of ensuring information assurance practices were being
9 followed by the brigade?

10 A Yes, sir.

11 Q You were in charge of ensuring any required
12 training on information assurance was being done by the
13 brigade?

14 A Yes, sir.

15 Q Other than the online IA security training
16 that everyone does, did you do any additional training
17 while deployed on IA, information assurance?

18 A Posted flyers and bulletin, and on bulletin
19 boards and little reminders, you know, don't use thumb
20 drives, security is your responsibility and little
21 reminders around the brigade headquarters, but no

1 formal training, no, sir.

2 Q And that applied to the brigade as a whole,
3 correct?

4 A Yes, sir.

5 Q Now, I want to ask you a little bit about
6 the shared drive. That's the T-drive, am I right?

7 A Yes, sir.

8 Q The T-drive was authorized to store up to
9 secret information?

10 A Correct, sir.

11 Q And users were permitted to basically save
12 information on the T-drive if they wanted to?

13 A Yes, sir, it was available for any user on
14 the domain to share or store information.

15 Q And obviously a user might do this if they
16 wanted to have something on the shared drive and if it
17 was lost by, because their computer crashed, they would
18 be able to go to the shared drive; is that right?

19 A That is one use of it, yes, sir.

20 Q And there was no limitation on the amount
21 of classified information that you placed onto the

1 T-drive; is that right?

2 A The only limitation would be the physical
3 storage limits of the device itself. It didn't place
4 any limits on individuals.

5 Q Was there any limitation on the type of
6 classified information that you stored on the T-drive?

7 A Yes, sir. You could only store up to
8 secret.

9 Q If it were secret, you could store it on
10 the T-drive?

11 A Yes, sir.

12 Q As the brigade IM, was there any limitation
13 on saving classified information onto CD if you wanted
14 to?

15 A At the time, no, sir.

16 Q I imagine if you did it, you put it on a CD
17 you would have to appropriately label it?

18 A Yes, sir.

19 Q And other than that, once you did that you
20 could do that with authorization?

21 A Yes, sir.

1 Q Now, as the IAM, information assurance
2 manager, you saw a little unauthorized media on the
3 T-drive?

4 A Correct.

5 Q You saw this media basically on a regular
6 basis?

7 A Yes, sir.

8 Q And the unauthorized media included music?

9 A Yes, sir.

10 Q It included movies?

11 A And games, yes, sir.

12 Q And games?

13 A Yes, sir.

14 Q And the games were executable files,
15 correct?

16 A They are, sir.

17 Q Did you see other executable files besides
18 games?

19 A Not that I recall, no.

20 Q Do you recall seeing mIRC chat on the
21 T-drive?

1 A Yes, sir.

2 Q Is that an executable file?

3 A No, sir, it requires installation.

4 Q So from your memory, mIRC chat on the
5 T-drive was not an executable file?

6 A No, sir.

7 Q Okay. Now executable file, let's talk
8 about that for a moment. They're programs that can run
9 without actually adding them to the computer. Am I
10 correct?

11 A Correct.

12 Q If you took a executable file and you put
13 it on the desktop of your computer and you double
14 clicked, it would run?

15 A Yes, sir.

16 Q And you wouldn't need admin. rights for
17 that?

18 A No, sir.

19 Q And the prosecutor said that some way you
20 could circumvent admin. rights, but with executable
21 files you're not circumventing admin. rights, correct?

1 A No, the file is designed that you don't
2 install it. There's nothing that shows that you need
3 administrative rights to run it or operate it. It just
4 executes its commands.

5 Q And if you didn't want to put on it your
6 desktop, you could run an executable file from a CD as
7 well, couldn't you?

8 A You could run it from a CD, a flash drive,
9 from the T-drive, anywhere you could get access to it.

10 Q And Wget, I know you said you became
11 familiar with that program as part of this case?

12 A Yes, sir.

13 Q But Wget is an executable file, right?

14 A Yes, sir.

15 Q And if, if a soldier wanted to run Wget
16 from a CD, they didn't need admin. rights for that?

17 A No, sir.

18 Q If they wanted to run it from the desktop
19 of their computer, they didn't need admin. rights for
20 that?

21 A No, sir.

1 Q Now, from your position as the IAM, was
2 there any kind of S6 Captain Cherepko authorized
3 movies, executable files, games, folder on the T-drive?

4 A No, sir.

5 Q So the Colonel, Colonel Miller, he was your
6 brigade commander?

7 A Yes.

8 Q Did Colonel Miller say here's the NWR
9 folder Captain Cherepko approved of, it has music,
10 movies and games and mIRC chat that we have approved it
11 and, you know, go through and use it?

12 A No, sir.

13 Q So that was never done?

14 A No, sir.

15 Q As the brigade IAM, I imagine you would
16 know this but did Colonel Miller ever come to you and
17 say I want to authorize mIRC chat on my D6-A computers?

18 A No, sir.

19 Q Did he ever say, hey, we need to put
20 together a letter that says, I know mIRC chat is not
21 part of the baseline program for D6-A, but I want to

1 take on the responsibility of getting it on my D6-A
2 computers because it's mission essential?

3 A Sir, I was not involved with D6-A
4 configurations or management at all so if that were the
5 case, I would have not been able to comply with his
6 request. But no, he did not, never asked me for that.

7 Q And being a staff officer myself at
8 different times, I imagine if the brigade commander
9 wanted to do something, he would first go to you, his
10 staff officer, who is basically in charge of that type
11 of stuff to talk to you about it?

12 A Most likely he would have gone to my
13 supervisor first, sir.

14 Q That would be Major Morrow?

15 A Yes, sir.

16 Q And I imagine that that would be batted
17 around with you then at some point?

18 A Yes.

19 Q Do you recall at any point Colonel Miller
20 talking about adding mIRC chat to D6-A computers?

21 A No, sir.

1 Q Now, whenever you saw music, movies and
2 executable files on the T-drive, you would remove it,
3 correct?

4 A I would; yes, sir.

5 Q And everyone, even though you deleted these
6 files, they would come back into the T-Drive?

7 A Yes, sir.

8 Q So users would add it back onto the
9 T-Drive?

10 A Yes, sir.

11 Q And I'm correct then this was not something
12 that was leftover from the previous brigade 3A2?

13 A I may have been.

14 Q When it was deleted and put back on
15 obviously 3A2 wouldn't put it back on?

16 A No, but it still may have been remnants
17 from 3A2 if it was a local machine and they were copied
18 from a local machine or if they were copying it to a CD
19 and moving it back; but no, 3A2 did not.

20 Q When it got back into the T-drive, that was
21 from somebody in your brigade?

1 A You could make that assumption; yes, sir.

2 Q Would you make that assumption?

3 A I would, sir.

4 Q Now, you alerted your command to the
5 presence of unauthorized media on the T-drive?

6 A I did.

7 Q You notified your immediate supervisor,
8 Major Morrow?

9 A Yes, sir.

10 Q You also notified Lieutenant Kearns?

11 A Through Major Morrow.

12 Q You told them about the presence of
13 unauthorized media on the T-drive?

14 A I did.

15 Q You told them about the practice of placing
16 the unauthorized media on the T-drive and it needed to
17 stop?

18 A I did. And I also explained the reasons
19 why.

20 Q That was because you viewed it as an
21 information assurance threat?

1 A Yes, sir.

2 Q And to your knowledge, nothing was done by
3 the chain of command to act upon what you said?

4 A The command agreed that the practice needed
5 to stop.

6 Q But nothing was done?

7 A I don't know that they did or did not take
8 any actions on it. I just know that the practice
9 didn't stop.

10 Q You know what?

11 A That the practice of putting information on
12 there didn't stop.

13 Q And in fact it didn't stop until you
14 unplugged the network to redeploy?

15 A That would be about the time; yes, sir.

16 Q To your knowledge, was there ever anyone
17 punished for placing unauthorized media on the T-drive?

18 A Not that I know of, sir.

19 Q If a member of the brigade came to you and
20 said Captain Cherepko, I've got a mission essential
21 program that I need to install on my computer, what

1 would be the process for you to get that done?

2 A It depends on the software and whether I
3 have it, it's authorized, and I have a license allowing
4 me to legally use it, if I have approval, the software
5 and a license, then I would just install it.

6 If I did not have one of those things, I
7 would then investigate the process of obtaining one of
8 those three, the missing piece of the puzzle.

9 Q And have you ever had a situation where you
10 had to go through that approval process of trying to
11 find the --

12 A Yes, sir.

13 Q -- approval?

14 A Oh, approval?

15 Q Correct. Something that you didn't already
16 have approval for?

17 A No, sir; only I didn't have a license so I
18 had to purchase it.

19 Q And do you even know the process of how
20 that would happen if you didn't have a license for it
21 and there was not approval for it?

1 A If I didn't have a license, I would simply
2 go to the S4 and begin the process to purchase one. If
3 I didn't have approval, I would call up the G6 division
4 and begin the process required to obtain approval to
5 use the software.

6 Q I don't want to go through the whole
7 process, is that a long process?

8 A It's not short; yes, sir.

9 Q Have you ever successfully gone through the
10 process where you went through the G6?

11 A I have not.

12 Q Have you ever heard of anyone going through
13 the process to get approval through the G6?

14 A Not personally. I can assume that it has
15 happened because there are hundreds of programs that
16 are approved. I don't know of anyone who has actually
17 done it.

18 Q Okay. Now, with regards to the IAM
19 program, I think we understand that only an administrator
20 can actually add the program, right?

21 A Yes.

1 Q But with a executable file, were you aware
2 whether or not soldiers were adding executable files to
3 the desktop of their computer?

4 A I was not. Other than games that I was
5 find on the T-drive, no, I was not aware of any other
6 executable files.

7 Q When you say games, games would function
8 much like Wget or any other executable file that once
9 you click on it, it actually starts to run?

10 A Not all, but most.

11 Q So some games would function the same way
12 as Wget would?

13 A Some would.

14 Q Were you aware of whether or not anyone in
15 the unit, soldiers in the unit, believed that they
16 could add games, music, executable files, like, they
17 were given approval to do that?

18 A No, sir. Everyone signed the document that
19 said they would not add software or change the
20 baseline. And beyond that, no one that I know ever
21 told them that they were and none of the officers or

1 NCOs that I knew personally thought that it was
2 acceptable.

3 Q But am I correct in saying it wasn't very
4 hard for you to search the T-drive and find executable
5 files, find music and movies?

6 A No, sir; it was not.

7 Q Pretty much any day you wanted to, you
8 could go look and you would find it?

9 A More or less; yes, sir.

10 Q And even though that was the case, to your
11 knowledge that stuff never came off of the T-drive, the
12 music, movies and games, it never came off the T-drive
13 until you basically unplugged?

14 A No, sir. It would disappear for short
15 periods of time after I found it and deleted it and
16 then it would reappear hours, days, week, months later.
17 But for a brief period of time, it was free of all
18 unauthorized media.

19 Q So every kind of soldier and NCO you knew
20 understood that it was not appropriate, correct?

21 A Correct.

1 Q Did you ever get to the bottom of who was
2 adding all this stuff under the T-drive?

3 A Whenever I was able to identify a soldier
4 who was doing, adding the media, I would go to that
5 soldier, explain the reasons why it's a bad idea. I
6 would explain to their first line supervisor why it was
7 a bad idea and then I would leave it up to their chain
8 of command to pursue the, whatever they wanted to do to
9 the soldier.

10 Q To your knowledge, was anything ever done
11 by the chain of command?

12 A Not that I know of.

13 Q Let's talk about access controls on the
14 shared drive. Do you know why none of the files on the
15 T-drive were encrypted?

16 A It was a secure network. There was no need
17 to encrypt the files.

18 Q So any file on the T-drive, video or
19 otherwise, would be unencrypted?

20 A Yes, sir. Unless the user opted to encrypt
21 the file for some reason.

1 Q Do you know why none of the information on
2 the T-drive was compartmentalized?

3 A It was, it was compartmentalized into
4 folders, but there was no restrictions on who could
5 access the folder, if that's what you mean.

6 Q That is what mean. So, in other words, if
7 I had access to the T-drive, I had access to everything
8 on the T-drive?

9 A Yes, sir. Unless there was a restriction
10 requested. If a soldier or a staff officer or someone
11 would come to me and request a restriction on a file or
12 folder, I would initiate that restriction.

13 An example I can give you the S3 shop did
14 not want anyone to be able to modify the long range
15 planning calendar so I put a restriction that only one
16 master sergeant could edit that document. Everyone
17 could view it, but only he could edit it.

18 If you asked for it, I gave it to you. But
19 I don't make the decision on what you do and what the
20 S3 does and does not want restricted.

21 Q Was that hard to do, if you wanted to put

1 restrictions to limit access to certain information on
2 the T-drive, is that a difficult thing for you to do?

3 A For me to do, no, sir. For the users, yes.

4 Q Now, I want to talk about the use of
5 executable files on the desktop of a computer.

6 A Okay, sir.

7 Q We established that you don't need admin.
8 rights to do that. But from your position as the IAM
9 could computers be configured to where that would not
10 be a process that you could do, that you couldn't put
11 an executable file on the desktop of a computer?

12 A There are systems that exist that would
13 alert you, not the user, but would alert the
14 administrators to the use of executable files and would
15 not allow them to run, yes.

16 Q I know you weren't in control of the D6-A,
17 but for your computers, if you wanted to, and say for
18 any S6 computer we want to make sure no executable
19 files are run, could you have prevented that from
20 happening?

21 A No, sir.

1 Q Why not?

2 A I did not have the system that the Army has
3 purchased to prevent those types of events from
4 occurring.

5 Q So it was a resource thing for you?

6 A Yes, sir. I had not been issued, HPSS
7 system that does that.

8 Q But that was possible, if you got resource
9 of that system you could prevent somebody from using
10 executable file; is that correct?

11 A More or less. It would be possible if I
12 was given the system and we had the training and the
13 understanding to properly employ the system.

14 Q Okay. Let's talk about access controls on
15 the SIPRNET. All right?

16 A Sure, sir.

17 Q Other than information that might be
18 password protected, were there any access controls on
19 the SIPRNET that you're aware of?

20 A I'm not sure what you mean, sir.

21 Q If I had SIPRNET access like I was a person

1 who had the clearance, had a computer hooked up to the
2 SIPRNET, was there any limitation on what I could go
3 see on SIPRNET?

4 A Yes, sir.

5 Q And what was that limitation?

6 A There are probably hundreds, if not
7 thousands of locations on SIPRNET that you would not be
8 able to go to.

9 Q Because of why?

10 A Being a member of the 2nd Brigade, 10th
11 Mountain you had, your authorization were based on
12 being a member of my domain. As a member of my domain,
13 you could not go to the, you know, M and D north sites
14 or their shared drive or shared point portal and access
15 anything because I did not have a trust relationship
16 configured in my extractor that allowed us to share
17 information, that sort of matter.

18 You could not go to Afghanistan site shared
19 drive or any location and pull information unless we
20 had a trust established. Or, if they had that
21 alternate distance site configured in such a manner

1 that you did not require verification of your
2 authenticity.

3 Q I want to break it down. If I'm
4 understanding you right. I could go on at a SIPRNET
5 computer on your domain, I could go to any place that
6 you had a trust relationship with?

7 A Inside my domain you could go to any, you
8 can go to SharePoint portal. You could go to, you can
9 go to the T-drive. You can go to any of the locations
10 we had that were available to general users.

11 We had some locations that were completely
12 restricted to administrators that no one had rights to
13 but myself, my NCO, warrants and a few other guys.

14 But as a general user, you could go to
15 anywhere within my brigade that was not specifically
16 prohibited.

17 Q And --

18 A Outside of the domain, outside of the
19 brigade we'll say, you could not go to 1st Brigade 3rd
20 ID, you could not type in their address in the URL bar
21 and bring up their site and access any information

1 unless they specifically configured their systems to
2 allow visitors. If you allow visitors then anyone can
3 have access to what you give visitors access to.

4 And that goes for every other unit on
5 SIPRNET in the world.

6 However, my brigade, because we work
7 closely with certain units, we had a trust established,
8 which means I trust all of their users, meet the
9 requirements, they trust all my nets, that's the
10 general term. The trust is actually the connections
11 that allows anyone in their domain access to mine and
12 allows anyone in mine access to the far domain.

13 We had trust established with several of
14 the other brigades in the M and DB area and with
15 multinational brigade and because we had Corp. level
16 assets on my network that I managed with MNFI.

17 Q So if I could access something on SIPRNET
18 on your domain then if I could access it, I was
19 permitted to go there?

20 A I think you have that backwards, sir.

21 Q Based upon what you said, everything you

1 said --

2 A If you had access and it was not
3 specifically restricted, you had the ability to go
4 there. You may not have had the authority to go there.
5 Having the ability to go somewhere doesn't mean you
6 have the need to know or the authority to go there.
7 But you have the ability to go there and view, edit,
8 remove documents.

9 Q All right. So I'll try to simplify it.

10 A Okay. Sorry, it's very complex.

11 Q I'm trying to make it easy.

12 If I go, if I can go on the SIPRNET
13 computer, if I can go to a place on your domain, then I
14 have at least access to it, access to go there,
15 correct?

16 A You have the -- there's no technical
17 restriction preventing you to go to Captain Tom
18 Cherepko's folder, view, edit, remove documents.

19 Q Then there is the separate thing you talked
20 about that you might have access but, and ability to go
21 there, but maybe not the authority to go there, is

1 that --

2 A Yes, sir. For example, I have the ability
3 as administrator to go anywhere. But I have no need to
4 go to the medical officer's file and view people's
5 medical records. I have no real need to do that and no
6 authority to do that.

7 Q And were you aware of whether or not
8 all-source analysts were basically told they could look
9 at anything they wanted to that they had access to?

10 A I don't know what they were told, sir.

11 Q So that would be a no then?

12 A No.

13 Q And when you say the ability and the
14 authorization, if you had the ability to go there
15 because of your domain allowing you to go there and you
16 had the authorization from your supervisors to go
17 there, were there any other restrictions on access?

18 A There were no technical restrictions that
19 we did not apply. There was no --

20 If your supervisor told you to go into the
21 S4 folder and find how much fuel the brigade uses in a

1 three-month period and you worked in the medical
2 company, you could do it.

3 Q With regards to the stuff that PFC Manning
4 had access to, did he have to gain access to that
5 information on the SIPRNET by hacking anything?

6 A Inside my domain or outside my domain?

7 Q Inside your domain.

8 A I would say no, sir.

9 Q Did he need to break any encryption or
10 anything to get access to anything that was inside your
11 domain?

12 A No, sir.

13 Q Did he need to circumvent anything to get
14 access to something that was inside your domain?

15 A He would have needed to circumvent nothing
16 technical.

17 Q So maybe the only restrictions might be if
18 he had authorization from a supervisor to go, using
19 your example, if I'm in the medical area, I might not
20 have a reason to go to S4C or fuel consumption for the
21 brigade so even though I have access to it, I might not

1 have the authority to go there unless my boss said, you
2 know what, it's important to me, find out how much fuel
3 we're using, we want to tell them how much medical
4 needs?

5 A That would be a fair assessment; yes, sir.

6 Q Now, I want to ask you about being the IAM
7 and, as far as going to the brigade, was this your
8 first duty assignment as an IAM?

9 A Yes, sir.

10 Q And my understanding is you basically, was
11 this your first brigade automations officer position as
12 well?

13 A It was, sir. It was my first duty position
14 out of the schoolhouse.

15 Q And at the time that you got there, were
16 you aware that the IAM was responsible for verifying
17 that all computers under their oversight were properly
18 certified and accredited?

19 A I was not, sir.

20 Q And as part of that process were you aware
21 that you had to submit what's called a DIACAPP package?

1 A I was not, sir.

2 Q And my understanding that's a Department of
3 Defense Information Assurance Certification and
4 Accreditation Process Packet; is that right?

5 A Sounds about right, sir.

6 Q Your brigade was required to basically
7 submit one of those packages, correct, the DIACAPP
8 package?

9 THE COURT: What is it?

10 MR. COOMBS: Delta, India, Alpha, Charlie,
11 Alpha, PaPa.

12 Q Did your brigade submit the required
13 DIACAPP package?

14 A Not that I know of sir.

15 Q And that DIACAPP package was basically
16 designed, supposed to be designed to ensure that there
17 was a disciplined method for information assurance?

18 A Sir, the systems that we had in place at
19 FOB Hammer were relatively new to the brigade before
20 they deployed and certification and accreditation is
21 valid for three years so there would have been no need

1 to submit one at that point.

2 Q Are you aware of whether or not somebody
3 higher than your brigade disagreed with that
4 determination you just made?

5 A I am, sir.

6 Q And did they disagree with that
7 determination?

8 A They did, sir.

9 Q And so the DIACAPP package, going back to
10 my question, that was supposed to ensure a, basically a
11 discipline method for information assurance within the
12 brigade?

13 A It is the paperwork showing that the
14 security implementations that are required that I had
15 in place were in place.

16 Q To ensure basically a discipline
17 information assurance environment?

18 A It's the paperwork that just shows that
19 what's required to be in place is in place.

20 Q And I'm sorry, I don't mean to be aloof,
21 I'm trying to get an answer to this part that that

1 process then is to ensure that you have a discipline
2 information assurance environment. That you're doing
3 everything you're supposed to?

4 A I'm not sure what the regulation or
5 textbook answer is, sir, but the purpose of it is to
6 validate that all of the requirements I have done.

7 Q And those requirements, what's the purpose
8 for those requirements?

9 A To provide security for the network.

10 Q Thank you.

11 MR. COOMBS: No further questions.

12 MR. WHYTE: One minute, Your Honor.

13 THE COURT: Yes.

14 REDIRECT EXAMINATION BY MR. WHYTE:

15 Q Captain Cherepko, you said you monitored
16 the network to see if there were any movies, music and
17 games on the computer?

18 A I did, sir, for the most part I delegated
19 to IANCO but occasionally I did it personally.

20 Q How often would you search the network for
21 unauthorized programs?

1 A Personally?

2 Q Yes.

3 A When I had free time.

4 Q So not every day?

5 A No, not every day.

6 Q Why not?

7 A Because I had a -- I had an IANCO who
8 performed the task and more importantly everyone on the
9 network had a security clearance and signed the
10 agreement that they wouldn't do unauthorized things so
11 I didn't feel the need to search every moment of every
12 waking day.

13 Q Why is that?

14 A Because everyone was trusted to do what
15 they said they would do.

16 Q So defense on cross asked you about
17 accreditation for the network?

18 A Yes, sir.

19 Q If the network were actually accredited --

20 A I believe it was, sir.

21 Q -- okay, what would prevent a soldier from

1 actually burning classified information from the
2 network?

3 A The accreditation is paperwork, sir, that
4 stops someone from doing nothing.

5 Q What about leaving the SCIF, for instance,
6 with classified information?

7 A That would not prevent it; no, sir.

8 MR. WHYTE: No more questions, Your Honor.

9 MR. COOMBS: Nothing for me, ma'am.

10 THE COURT: I have a couple of questions.

11 EXAMINATION BY THE COURT:

12 Q With respect to the movies and the games
13 that you talked about that were on the T-drive, do you
14 remember were they on there when you arrived, at least
15 were some of them on there from prior units?

16 A They were. The T-drive had been inherited
17 from several previous units over several years and they
18 were there from the day we arrived. You could go
19 almost to any folder from the Brigade 2nd Airborne and
20 find funny movie clips, music.

21 Q You testified that those were unauthorized

1 programs and files on the -- would you consider a game
2 or music, were they programs?

3 A The movies and music are media that require
4 a program to operate. Unless they've been tampered by
5 people with mal intent to do executable things in the
6 background and that's the main security threat for
7 them. They can be modified to do security violations
8 that you don't know about.

9 Q The T-drive, did the network contain a
10 program to operate them?

11 A The movies?

12 Q Yes.

13 A Yes, ma'am.

14 Q And the music as well?

15 A Yes, ma'am. The Microsoft Windows media
16 player would play movies and the music.

17 Q What about the games?

18 A The games were either independent
19 executable files or they were scripts written inside of
20 Excel spreadsheets or Word documents. Those sorts of
21 programs that would run those.

1 But the majority of them were independent,
2 executable files that required nothing but the one file
3 that you would double click on and run.

4 Q You testified earlier that you would go to
5 the T-drive and remove the music and the games and the
6 things that were unauthorized. Other than yourself,
7 was there -- you said they kept reappearing, was there
8 in your opinion a command laxity about enforcing this?

9 A In my opinion, ma'am?

10 Q Yes.

11 A More or less, yes.

12 You know, we alerted the command to the
13 presence of it. The reasons for why it is unacceptable
14 for being there, both regulatory and security-wise, why
15 they're not allowed to be there, but yet they continued
16 to appear.

17 I tried to use the analogy they are a
18 information security negligent discharge. While you
19 may assume that firing a weapon into a barrel doesn't
20 hurt anyone, you never know.

21 Q Did anyone in the chain of command tell or

1 indicate to you why they were sort of letting this go?

2 A No, ma'am.

3 THE COURT: Any followup based on that?

4 MR. COOMBS: The defense rests, ma'am.

5 MR. WHYTE: Maybe two questions, Your
6 Honor.

7 THE COURT: That's fine.

8 CONTINUED REDIRECT EXAMINATION BY MR. WHYTE:

9 Q Captain Cherepko, were you aware of any
10 freeware on the network, a freeware? You testified
11 earlier that freeware was specifically prohibited under
12 25-2, were you aware of any freeware on your network?

13 A One could make the argument that the games
14 they found were freeware.

15 Q Did you find with looking through the
16 network in the unauthorized executable files outside of
17 games?

18 A No, no, sir.

19 Q Did you notify the command of anything
20 other than music, games, movies on the network?

21 A On the network? Just general IA violations

1 that I found. An example is one of the FOB's we had an
2 Iraqi Army unit and they tried to splice into my fiber
3 with copper, which would never work, but it's still an
4 IA violation. So I alerted them to that as well.

5 Every IA violation I found I reported to
6 the command.

7 MR. WHYTE: Thank you.

8 MR. COOMBS: Just a couple questions based
9 upon that.

10 CONTINUED RECROSS EXAMINATION BY MR. COOMBS:

11 Q Were you looking for executable files on
12 the T-drive?

13 A Yes, sir.

14 Q And how were you looking for them?

15 A I would do a search for all files that end
16 in dot EXE, dot VAT, dot VBS, all the types of
17 executable files.

18 Q Are you familiar with media player VLC?

19 A I am.

20 Q Did you find that on the T-drive?

21 A Yes, sir.

1 Q And was that an authorized media player?

2 A I believe it was; yes, sir.

3 Q What do you base that on?

4 A I recall, I believe I recall looking to
5 find out if it was authorized because it was there and
6 people were wanting to use it. And they were wanting
7 to upgrade to the newest version and it's version
8 specific, so.

9 MR. COOMBS: Thank you.

10 THE COURT: Go ahead.

11 MR. WHYTE: One question.

12 CONTINUED REDIRECT EXAMINATION BY MR. WHYTE:

13 Q When you searched the network for any
14 music, games, would you actually be looking at a
15 person's desktop as well?

16 A No, sir. I did not have that ability.
17 Unless I walked to the desk and looked, but no.

18 THE COURT: I don't think I have any
19 further questions. Any last questions?

20 MR. COOMBS: Carry on.

21 THE COURT: Temporary or permanent excusal?

1 MR. WHYTE: Temporary, Your Honor.

2 THE COURT: You're temporarily excused.
3 Please don't discuss the case with anyone other than
4 trial counsel or the accused while the case is still
5 going on. You are free to go.

6 MR. WHYTE: Ma'am, the United States calls
7 Mr. Jason Milliman.

8 THE COURT: Are you all set to go without
9 recess? You ready to go, both sides?

10 MR. COOMBS: Defense is fine, Your Honor.

11 THE COURT: Proceed.

12 Whereupon,

13 JASON MILLIMAN,
14 called as a witness, having been first duly sworn to
15 tell the truth, the whole truth, and nothing but the
16 truth, was examined and testified as follows:

17 DIRECT EXAMINATION BY MR. WHYTE:

18 Q Your name is Mr. Jason Milliman from
19 Charlottesville, Virginia?

20 A Yes, sir.

21 Q What is your current military status?

1 A Retired.

2 Q When did you retire?

3 A August 31st of 2005.

4 Q How many hours did you serve in the
5 military?

6 A 21 years.

7 Q And what was your MOS when you retired?

8 A 33 Whiskey.

9 Q What is that?

10 A Electronic (INAUDIBLE).

11 Q Since you retired, what type of work have
12 you been involved in?

13 A Contractor.

14 Q Have you deployed as a contractor?

15 A Yes.

16 Q What was your first deployment as a
17 contractor?

18 A November of 2007.

19 Q And how long was that deployment?

20 A Until February of 2009.

21 Q Where were you stationed during this

1 deployment?

2 A Camp Slayer, Iraq.

3 Q What were your responsibilities at Camp
4 Slayer?

5 A I was a main hub FSE responsible for the
6 monitoring of all the D6-A servers throughout Iraq.

7 Q What is FSE?

8 A Field software engineer.

9 Q When was your second deployment as a
10 contractor?

11 A June of 2009.

12 Q And how long was that deployment?

13 A 18 months.

14 Q Where were you stationed during this
15 deployment?

16 A I went initially to JSS Loyalty then to FOB
17 Hammer and finished in Camp Ramadi.

18 Q When did you arrive at FOB Hammer?

19 A I think it was around September 2009.

20 Q And what unit were you with when you
21 arrived at FOB Hammer?

1 A 82nd.

2 Q When 82nd redeployed, what unit took their
3 place?

4 A 210 Mountain.

5 Q You were at FOB Hammer when 210 Mountain
6 arrived?

7 A Yes, sir.

8 Q Were you there when they finally redeployed
9 back to Ft. Drum?

10 A Yes, I was.

11 Q So you were there the entire time?

12 A Yes, sir.

13 Q What was your position at FOB Hammer with
14 210 Mountain?

15 A It was a different type FSE they called it
16 a fly away FSE. My job was based out of FOB Hammer to
17 support other units.

18 There was a main server at FOB Hammer and
19 all the users and laptops. They were stationed at --
20 wherever they were located, I fly to them and take care
21 of their machine as well.

1 Q So you're responsible for the D6-A
2 machines?

3 A Correct.

4 Q What is the purpose of a D6 machine?

5 A It's a suite of tools the intelligence
6 analysts use to gather the required data they need to I
7 guess exploit the intelligence.

8 Q And what network were these D6 machines
9 hooked up to?

10 A SIPR.

11 Q To your memory how many D6 machines were at
12 FOB Hammer?

13 A Roughly 35.

14 Q To access a D6 machine, did you have to
15 insert a Linux operating system?

16 A No.

17 Q Where did you work at FOB Hammer?

18 A In the SCIF.

19 Q How do you know PFC Manning?

20 A He was also in the SCIF.

21 Q What did you know about PFC Manning's

1 computer skills?

2 A Only what I heard, either him talk about or
3 others. I guess he had a computer business at some
4 point and he made a few comments about his skills.

5 Q What did PFC Manning say about his computer
6 business?

7 A I just remember at one point we talked
8 about problems and he said that if it was a problem
9 that was taking too long for his liking, he would
10 (INAUDIBLE) his machine until the customer couldn't fix
11 it.

12 Q What else do you know about PFC Manning's
13 computer skills?

14 A He made a couple comments. There was one
15 comment, there was no computer he couldn't hack into,
16 if people really knew what he would do with computers,
17 they would be amazed.

18 Q Did PFC Manning have issues with his
19 computer at FOB Hammer?

20 A Yes, he did.

21 Q And can you explain what those issues were?

1 A His co-user, Madaras was his name, he
2 approached me first. He was the day shift. Telling me
3 that his computer was acting funny.

4 MR. COOMBS: Objection, Your Honor.
5 Hearsay.

6 MR. WHYTE: Just a (INAUDIBLE) to elicit to
7 see what steps he took in response to the computer
8 problems that they were having.

9 THE COURT: Ask him if he learned if there
10 were computer problems yes or no and what he did.

11 BY MR. WHYTE:

12 Q Did you learn of computer problems?

13 A Yes, I did.

14 Q What did you do in response to those
15 computer problems?

16 A My standard steps are to have a user
17 recreate the problem in front of me so I can see what
18 symptoms there are and then troubleshoot from that
19 point.

20 Q What were some of those troubleshooting
21 tactics that you employed?

1 A Based on the symptoms that I was given I
2 tried to see if there was, first, fragmentation on the
3 drive that may have caused poor performance of the
4 applications so see if the hard drive was running out of
5 space, which may have been contributed to some
6 fragmentations as well. See if their user profiles are
7 corrupt and barring all of that, reimage his machine.

8 Q So if the profile became corrupt, how would
9 that happen?

10 A A lot of users would store everything they
11 had on their desktop and I explained to them it was
12 kind of like snow on the roof of your house. Your roof
13 is not meant for all the snow, eventually it's going to
14 cave in and crash. So they stored all of the data on
15 the desktop. It eventually would crash the profile.

16 Q What steps did you have to take if the
17 profile was corrupt?

18 A Usually they couldn't log in so I would
19 take another hard drive, take their hard drive out and
20 put another one in the place that had a similar
21 operating system, everything was exactly the same.

1 Pull the information from that hard drive like a USB
2 drive, you would pull it to the new drive and let them
3 start over.

4 Q Is this the reimaging process?

5 A Yes, I'm sorry, I'm nervous, that's the
6 reimaging process. But only a corrupt profile, I can
7 move the data to another folder, delete the profile,
8 have them log in and create another profile.

9 Q Do you remember what steps you took with
10 the PFC Manning computer?

11 A I do remember we had to reimage it several
12 times.

13 Q Can you explain what if this, again for the
14 court, what this reimaging process, literally the
15 soldier brings you the computer and what did you do
16 with it?

17 A After exhausting my other troubleshooting
18 steps, once I determined that the computer had to be
19 reimaged, I had a stack of spare drives. In the
20 interest of time so the analyst could get back to work,
21 I would take the old hard drive out and insert the new

1 hard drive and configure the network settings.

2 Once the computer was back up and running
3 as quickly as possible, I would then connect the old
4 hard drive to the new hard drive through the USB port
5 and universal hard drive adapter and get the data that
6 he or she had to have from that drive and transfer it
7 back to new drive.

8 Q And how often did PFC Manning have issues,
9 and I think it's Sergeant Madaras as well, how often
10 did they have issues with their computers?

11 A Much more frequently than anyone else.

12 Q Was PFC Manning authorized to repair the D6
13 computer?

14 A No.

15 Q Who was authorized?

16 A Just me.

17 Q So did you actually reimage their computer?

18 A Yes, I did.

19 Q How many times did you reimage their
20 computer?

21 A I don't recall exam how many times. I know

1 it was at least three.

2 Q Is that odd?

3 A It's odd.

4 Q Why? Can you explain why?

5 A Unless there's hardware failures, once a
6 machine is imaged, it's good until something drastic
7 happens to it.

8 If they run out of hard drive space causing
9 the operating system to crash or something or, you
10 know, if the hard drive fails itself, there's no need
11 to reimage the machine.

12 Q In your experience how long did it
13 generally take before it needed to be reimaged again?

14 A Manning's computer or others?

15 Q Others.

16 A In general, unless there was a hardware
17 failure or something catastrophic, it didn't.

18 Q When did PFC Manning and Sergeant Madaras
19 have computer issues during the deployment, at what
20 stage of the deployment?

21 A Shortly after 82nd left I remember Madaras

1 approached me first and a few other times after that
2 and relatively short order, like a month or so after
3 the previous reimaging.

4 Q And at that time in the deployment, how
5 many spare hard drives did you have?

6 A Probably five or six.

7 Q Was that, is that a lot or a little?

8 A That's probably relatively a lot.

9 Q Let's talk about administrator rights on
10 the D6 machine. Who had administrator rights on the D6
11 machines?

12 A I had rights and the mentor, his name is
13 Marvin Gammage (phonetic). He was the mentor.

14 Q So which soldiers of 210 Mountain had
15 administrator rights?

16 A None.

17 Q Did PFC Manning have administrator rights?

18 A No.

19 Q So what does it mean you were the
20 administrator of the D6 machines?

21 A You have full control of the machine.

1 Q So like what things can you do that an
2 ordinary user cannot do?

3 A If there was Google Earth or Microsoft
4 Office or something like that we installed, I could
5 install it with full rights and privileges without any
6 restrictions.

7 Q So was PFC Manning authorized to install
8 programs on the D6 machine?

9 A No, he was not.

10 Q What happened if a soldier wanted a program
11 for his D6 machine but it wasn't actually on the
12 computer?

13 A He needed, he or she, needed to contact me
14 and if it was an authorized program that I was allowed
15 to install, I would install it.

16 If I didn't know if it was authorized, I
17 would contact Camp Slayer lead FSE that was stationed
18 at Camp Slayer and make the request to him and usually
19 we were supposed to fill out an official software
20 request form but it was usually done word-of-mouth.

21 They were determined at Camp Slayer if it

1 was authorized and if it was they would tell me to load
2 it; if it was not, I couldn't load it.

3 Q When you were at FOB Hammer, were familiar
4 with Wget?

5 A No.

6 Q When you were at FOB Hammer, did any
7 soldier request permission to put Wget on their
8 computer?

9 A I do not recall anyone asking for it.

10 Q At FOB Hammer did you install Wget on any
11 D6 computer?

12 A Not that I can recall.

13 Q Are you familiar with what an executable
14 file is?

15 A I believe I am, yes.

16 Q What is an executable file?

17 A An executable file is something that runs
18 on its own. It doesn't require other files to operate,
19 I guess.

20 Q Are you familiar with the installation
21 process for an executable file?

1 A Relatively, yes.

2 Q What is that process generally?

3 A Normally it will have some sort of
4 interactive GUI telling you to do a certain process of
5 steps to install it. Normally for, like, Microsoft
6 Office or something, you would make modifications to
7 system files or registry, that kind of thing.

8 Q Is Microsoft Office an executable file
9 itself is an executable file?

10 A I don't know that I know the correct answer
11 to that. I'm just using that as an example to make
12 modifications to a file.

13 Q So could a soldier put an executable file
14 on their D6 machine?

15 A They could, but they wouldn't be
16 authorized.

17 Q Who was authorized to put executable files
18 on the D6 machines?

19 A Just me or other FSEs.

20 Q How would using an executable file allow a
21 user to circumvent and he would actually contact you?

1 A Can you say that again?

2 Q How would using an executable file
3 circumvent the need to come to you, the administrator?

4 A If I understand the question correctly, a
5 user could install the executable file on the desktop
6 without coming to me even though it wouldn't be
7 authorized?

8 Q When you were at FOB Hammer, was Wget an
9 authorized executable file?

10 A I don't recall but I don't believe so.

11 Q Do you know if PFC Manning had Wget on his
12 computer?

13 A I do not know.

14 Q You testified earlier that you were, you
15 were responsible for the D6 machines?

16 A Correct.

17 Q How did you not know if PFC Manning had a
18 program on his computer?

19 A I didn't go behind ever user on a daily
20 basis to find out if they had installed something. It
21 was understood or I thought it was understood that

1 we're all in a position of trust so that was not
2 something that was normally done.

3 MR. WHYTE: No more questions, Your Honor.

4 THE COURT: Cross-examination?

5 MR. COOMBS: Yes, Your Honor.

6 CROSS-EXAMINATION BY MR. COOMBS:

7 Q Mr. Milliman, how are you?

8 A Good, how are you?

9 Q Just a few questions for you.

10 I want to talk about some problems that the
11 D6-A computer had due to the environment, okay. Is
12 that all right?

13 A Yes, sir.

14 Q Now, heat was a major problems for the D6-A
15 computers, correct?

16 A In the beginning it was. But we overcame
17 that with some creative methods like using Gatorade
18 bottle caps to elevate it off the desktops to get more
19 air flow in there.

20 Q And the D6-A they would run hot even if
21 they were in an air conditioned room so you had to do

1 those kind of creative steps?

2 A Correct.

3 Q And in addition to heat, the dust from
4 being in the desert was a problem for the D6-A
5 computers?

6 A Correct. It was, very frequently it was,
7 it was required to frequently use cans of air to blow
8 the dust out of the machines.

9 Q That's what I was going to ask. You would
10 go around behind them and you would spray the
11 computers, basically to blow out the dust?

12 A A lot of cans of air; yes, sir.

13 Q Now, the computers still, in spite of doing
14 these things, the creative put a bottle cap underneath
15 or blow the dust, they would occasionally crash?

16 A Occasionally.

17 Q And with regards to the D6-A computers,
18 from your experience, there was usually always at least
19 two users on each D6-A computer; is that right?

20 A For the most part, I believe that's true.

21 Q Now, the D6-A computers, at least from the

1 users profiles, those could be corrupt if one or both
2 of the users were storing a lot of information on the
3 desktop?

4 A If one of the two users stored a lot of
5 information on the desktop only their profile would be
6 corrupt.

7 Q Yeah, I think you used an example of, like,
8 you know, snow --

9 A Right.

10 Q -- basically piling up on top of your roof
11 and caves in because of the weight?

12 A Correct.

13 Q So if one or both of the users were storing
14 a lot on the desktop, one or both of the user profiles
15 would become corrupt?

16 A One user couldn't make another user's
17 profile become corrupt because of what they did to
18 their profile.

19 Q So it would only be the user profile that
20 had too much information that would be corrupt?

21 A Correct.

1 Q You talked about Madaras coming to you
2 complaining about his computer that he shared with PFC
3 Manning. It was Madaras coming to you to complain
4 about the computer, correct?

5 A Correct. He was the first one I saw
6 because he was on day shift.

7 Q It wasn't PFC Manning coming to you to
8 complain about the computer?

9 A I don't recall him -- he could have
10 complained but I don't recall. I just remember Madaras
11 because he was the first one I saw in the morning,
12 that's how it started.

13 Q And I guess you said sometimes you had to
14 reimage based upon the problems that you encountered?

15 A Correct.

16 Q Did you have to reimage the computer of PFC
17 Manning and Sergeant Madaras?

18 A Yes.

19 Q And again, that was based upon Sergeant
20 Madaras coming to you saying I've got problems with
21 this computer?

1 A The reimaging was based on my
2 troubleshooting, my diagnosis of what was the other
3 steps that had failed to correct the problem.

4 Q What precipitated the other steps was
5 Madaras coming to you, not PFC Manning?

6 A I believe so.

7 Q Now, whenever you would try to fix a
8 computer that crashed, sometimes you would retrieve
9 information, correct?

10 A You mean take their information that they
11 wanted to save and save it somewhere else?

12 Q Maybe that's a bad question.

13 If a computer crashed, sometimes you could
14 save all the information and sometimes you couldn't; is
15 that right?

16 A Sometimes I could save the user's data and
17 sometimes I couldn't, correct.

18 Q Okay. When you were looking I guess at
19 Sergeant Madaras and PFC Manning's computer, did you
20 ever look to see what they had on their desktop that
21 was causing the problems?

1 A Well, it's not always the desktop that is
2 the problem, but I would usually, the standard
3 operating procedure I guess you call it, I would see,
4 being the size of the desktop, if they had a large
5 amount of data I would say, hey, you need to move that
6 to My Documents folder. Otherwise you're going to have
7 a profile crash.

8 I would see if the hard drive is
9 fragmented. I would see if they were running out of
10 hard drive space.

11 And if those things all seemed in order and
12 I couldn't find another way to fix the problem, I would
13 give them an opportunity. I could tell them I can
14 delete your profile and recreate a new one or I can
15 reimage your machine. And usually they would just opt
16 to have the machine reimaged and skip that step.

17 Q At least the time that you reimaged the
18 computers from your memory, I know it's been a while,
19 but from your memory it was Madaras asking you to
20 reimage the computers and not PFC Manning?

21 A I don't know 100 percent who requested but

1 I would say probably Madaras.

2 Q Okay. I want to ask you a few questions
3 about adding software to the D6-A computer. All right?

4 A Sure.

5 Q And I believe you said on direct that you
6 were the only one authorized to do that?

7 A Correct.

8 Q So if somebody wanted something they would
9 come to you and say Mr. Milliman, could I please add or
10 could you add this software onto my D6-A computer?

11 A Correct.

12 Q And they would do that because you were the
13 only one in addition to another civilian that had
14 administrator rights on those D6-A computers?

15 A Correct.

16 Q If you were asked to put a program onto the
17 D6-A computer could you tell us what the process was
18 that you would go through in order to determine that
19 yes, I will do that, or, no, I won't do that?

20 A If a user approached me requesting a
21 program to be loaded onto the D6-A that wasn't part of

1 the baseline, for instance there was a compression
2 program that they use as a standard tool. And at the
3 first request I didn't know it was authorized or not,
4 so I would contact the lead FSE, field software
5 engineer, at Camp Slayer, who would then either be able
6 to give me a direct answer, or if he didn't know the
7 answer he would find out the answer and get back to me
8 whether it was authorized or not.

9 If it was authorized I would install it; if
10 not I wouldn't.

11 Q Was there ever a time where -- do you
12 remember the brigade commander for the 210 Mountain, do
13 you remember who that was?

14 A No, I don't.

15 Q Does Colonel Miller sound familiar?

16 A Yes and no. It's a very common name but I
17 don't recall that being the commander.

18 Q Do you recall a time wherein the brigade
19 commander came to you and said, I want to get mIRC chat
20 on to my D6-A computers?

21 A I don't recall it but it's quite possible

1 that it happened.

2 Q Do you recall ever the brigade commander
3 signing a form saying I want the D6-A computers to have
4 mIRC chat, I'm going to take responsibility for that
5 because it's not part of the baseline package. Here's
6 the form, go make it happen.

7 A I don't recall that series of events but I
8 know there were letters and the standard -- we had like
9 a little book of memorandums and letters from certain
10 folks accepting risk and so forth.

11 I know that mIRC chat was not on the
12 baseline, the standard baseline for D6-A but it was
13 granted authority because it was the tool of choice for
14 both the 82nd and 210th Mountain Division and other
15 units as well. So they stopped using the D6-A
16 collaboration tool and started using mIRC chat. So it
17 was common for me to load mIRC chat on D6-A.

18 Q So when you did that from your memory, I
19 know it's been a while, but based upon your memory,
20 that wasn't at the request of the brigade commander?

21 A I would say that's a fair statement. I

1 don't recall that being directly from the brigade
2 commander.

3 Q And mIRC chat, the D6-A computer had as
4 part of its baseline package a program called cyb jabber?

5 A Say it again?

6 Q Right. For the baseline package for mIRC
7 chat, the collaborative tool, the communication tool
8 that they had was cyb jabber; is that correct?

9 A I think cyb jabber was a collaboration tool
10 for D6-A.

11 Q That's what I mean.

12 A Yeah, I think mIRC chat was a collaboration
13 tool they wanted to use instead of cyb jabber.

14 Q Exactly. So they were asking you to put
15 something on that was not the baseline tool --

16 A Correct.

17 Q For the D6-A computer?

18 A Correct.

19 Q And from your memory then you were the one
20 adding mIRC chat to anybody's computer that asked for
21 it, based upon once you got approval?

1 A When I first deployed my second deployment
2 as a fly away FSE with the 82nd was my first
3 introduction that I recall of mIRC chat. So I went
4 through the same steps I described earlier.

5 Contacted the lead FSE at Camp Slayer.
6 They determined it was a authorized program to be
7 installed so from that point on I would install it.

8 So when I would reimage a machine or when
9 the 210 Mountain came in, it became a standard tool
10 that I installed in all the D6-A machines.

11 Q When you installed it on all of the
12 machines, there would be no need for PFC Manning then
13 to go to somebody's computer and put mIRC chat on their
14 computer?

15 A That's correct.

16 Q And at least from your business, if PFC
17 Manning was asked to put mIRC chat on somebody's
18 computer, that would not have been something you would
19 have approved of?

20 A Correct.

21 Q I know you used the example of an

1 executable file, I just want to make sure that we will
2 have a common understanding of that.

3 If I had an executable file and I wanted to
4 put it on my desktop, something that I double click and
5 it ran, could I do that, not from the standpoint of
6 approval, but could I do that as far as the ability to
7 do it?

8 A Yes, the ability is there although the
9 authorization is not.

10 Q And from your position, if the D6-A
11 computers, if you wanted to, could you position the
12 D6-A computers in such a way to prevent a person from
13 having the ability to put an executable file on the
14 desktop?

15 A I believe the only way to restrict that to
16 take away all the privileges of the user to write to
17 their own desktop. I think that would severely impact
18 the analysts mission.

19 Q So from your position and knowledge, there
20 was no way to prevent somebody from putting an
21 executable file on the desktop short of eliminating

1 their ability to write anything to the desktop from?

2 A My opinion, yes.

3 Q Obviously that didn't happen because the
4 soldier had the ability to put stuff on their desktop;
5 is that right?

6 A Yes.

7 Q And because they could put it on their
8 desktop, if a soldier wanted to they could put games,
9 music, movies and executable files on their desktop?

10 A That's true.

11 Q Now, in the past you had noticed that
12 soldiers had, in fact, placed music on their D6-A
13 computers?

14 A Correct.

15 Q And games as well?

16 A I can't say for certain the 210 did. I
17 know other units had, but I can't recall if the 210th
18 did or not.

19 Q And having games and/or music or executable
20 files or whatnot on your D6-A computer, that wasn't
21 allowed?

1 A It was not authorized.

2 Q From your position?

3 A From my position, yeah.

4 Q But even because you didn't think it was
5 allowed, you didn't feel that you were in the position
6 to tell the soldier, hey, take that off your D6-A
7 computer?

8 A I had no authorization to tell a user what
9 to put or remove from the computer. I can only make
10 suggestions.

11 Q When you made suggestions, I imagine you
12 might make suggestions to the soldier and then their
13 immediate supervisor?

14 A Correct.

15 Q And then whether or not the soldier or
16 supervisor chose to follow your suggestions, you
17 wouldn't know at that point?

18 A Yeah, that's not for me to know.

19 Q And I know you said you weren't making it a
20 habit of looking at what soldiers were and were not
21 placing on their D6-A computers?

1 A Right. The only time I would see the
2 computer is when I had to provide updates to the
3 operating system or security patches or if I had to
4 reimage the machine.

5 Q So based upon that I guess you wouldn't
6 know how prevalent, if at all, it was for soldiers to
7 put executable files on their D6-A computers?

8 A Correct.

9 Q Now, based upon your experience, you did
10 have situations where in the past you had military
11 members trying to crack the password to the D6-A
12 computer?

13 A When there's a riptow, it was a common
14 occurrence --

15 Q I'm sorry to stop, the riptow is when two
16 units were swapping --

17 A Overlap. One would leave (INAUDIBLE).
18 Changes in authority. The new unit coming in would
19 bring in their D6-A. The standard philosophy I guess
20 or belief of the unit is they're our machines, we have
21 full rights, you can't have them as your privileges.

1 So there was a special letter signed by
2 somebody saying that only the D6-A FSE had
3 administrative privileges not the (INAUDIBLE). So in
4 the very beginning there was friction but we got that
5 ironed out so there were a couple of cases where they
6 would crack my password and remove the administrator
7 account and we would battle it out.

8 Q Essentially, my understanding is it was
9 basically you educating the military side of the house,
10 although you're using these computers and although
11 they're on your network, these are not your computers,
12 is that a fair statement?

13 A Not entirely. It was their computer but
14 because of the delicacy of the program and the suite of
15 tools it used, it required only the D6-A administrators
16 to be the ones to have the full administrator rights on
17 those machines.

18 Q So you would educate them, because of how
19 everything was set up, even though it's on your system,
20 you use it, technically it is your computer you pay for
21 it, but you don't have the ability to tinker with it?

1 A Correct.

2 Q Now, in the past also whenever you would
3 give or put mIRC chat onto a computer, it was a
4 specific version of mIRC chat; am I correct?

5 A I don't recall but it probably was.

6 Q Because authorization for programs was
7 version-based; am I not correct? You wanted to make
8 sure it didn't, it was compatible with everything else
9 so it had to be tested that particular version?

10 A Those tests would have been run by the FSEs
11 at Camp Slayer so I don't know and I don't think I can
12 speak to versions because I don't recall if there was
13 different versions of mIRC chat.

14 Q If you don't feel you can answer this you
15 can tell me I don't feel I can answer it and I won't
16 worry about it.

17 In your experience whenever you have got
18 approval for a certain program, was it a version-based
19 approval or was it for the lifetime, you could always
20 add whatever version you wanted of that particular
21 program?

1 A I think I can answer but it may be a
2 lengthy answer.

3 Q Go right ahead.

4 A We would have -- the Camp Slayer FSE's
5 would deliver new images to be used on D6-A machines.
6 Those images would contain, for instance, if there was
7 a new version of a program on that image, if a new
8 image or a new version of mIRC chat would be
9 authorized, it would come with notes saying now we're
10 using version B or C or whatever of this program, start
11 using this now.

12 We also had CDs that we carried that had
13 tools to use when we troubleshoot or other programs
14 that weren't on the standard D6-A baseline to load on
15 those user machines if needed, like the mIRC chat or
16 whatever.

17 So although I don't recall if there were
18 different versions of mIRC chat, it's possible. But it
19 would have been tested and vetted before it was allowed
20 to be installed.

21 Q So if I'm understanding correctly, if you

1 came back and you said version B is the one that's
2 approved and that's the one that is now the baseline,
3 that's approved, and we have got the version BCD; if
4 the following day I said, hey, Mr. Milliman I just
5 found out version C is available online, I'm going put
6 on it my computer, you would say no?

7 A Correct.

8 Q Okay. So that approval was then for that
9 version and if you had a newer version, you were not
10 supposed to put that on your computer?

11 A Not until it was authorized.

12 Q In your past experience you knew of
13 soldiers who liked to have the latest version of any
14 particular software, right?

15 A All soldiers like to have the latest
16 software but they didn't always get what they wanted.

17 Q Do you recall ever having a situation where
18 you did have soldiers putting more recent versions than
19 they should have on their D6-A computer?

20 A No, I don't.

21 Q You don't remember ever telling me about a

1 lieutenant who would do that because they liked having
2 the latest version of anything?

3 A I recall, I don't recall the rank, but I
4 recall an officer in the beginning getting the
5 compression program installed on his computer. And
6 that's when we had the password cracking and removing
7 of my (INAUDIBLE) account but I don't recall any other
8 instance than that.

9 Q So it was something early on when they put
10 something on and you basically told them hey, you're
11 not supposed to do this?

12 A Right.

13 Q Mr. Milliman, again, I appreciate your
14 time. Thank you.

15 THE COURT: Redirect?

16 MR. WHYTE: No questions, Your Honor.

17 THE COURT: I just have a couple.

18 EXAMINATION BY THE COURT:

19 Q Is mIRC chat an executable file?

20 A I think it is. I'm not an expert on it.
21 But from what I've read because it was one of the

1 questions that came up, it's a, it appears to be a
2 program that can be downloaded and installed directly
3 on your desktop.

4 Q When you had two users like Sergeant
5 Madaras and PFC Manning and one worked the day shift
6 and one worked the night shift, if, say, in this
7 situation Sergeant Madaras came up and said, I've got
8 all these problems with my computer, would you do the
9 reimaging before seeing PFC Manning on the night shift
10 or how did you do that?

11 A No, I made sure I tried to cover both
12 shifts. I would come in the middle of the day shift
13 and work through the rest of the day and half the night
14 shift as well so I can see both users and confirm the
15 problems with both users and make sure they were both
16 aware what was going on.

17 I wouldn't want to take the machine down
18 and possibly lose data without talking to both users to
19 find out what both users needed as data transferred
20 from one machine to another or one hard drive to another.

21 Q When you reimaged the machine of Sergeant

1 Madaras and PFC Manning, what did PFC Manning say about
2 his data, did he want it --

3 A They both wanted their data as far as I can
4 recall, but I can't recall specific conversation.

5 Q But they both wanted their data or all of
6 their data, was that typical?

7 A That was typical. Most users always wanted
8 their data. It was not uncommon.

9 THE COURT: Any followup based on that?

10 MR. COOMBS: No, ma'am.

11 MR. WHYTE: No ma'am.

12 THE COURT: Temporary or permanent?

13 MR. WHYTE: Temporary.

14 THE COURT: You are temporarily excused.

15 Please don't discuss your testimony or knowledge about
16 the case with anyone other than counsel or the accused.

17 THE WITNESS: Yes, ma'am.

18 MR. FEIN: Ma'am, the United States
19 requests a 10-minute recess.

20 THE COURT: Court is in recess until 1825
21 or 6:25.

1 (Brief recess.)

2 THE COURT: Let the record reflect all
3 parties present when the court last recessed are again
4 present in court.

5 The parties met with me briefly for an
6 RCM802 session and it appears they are working to
7 address other stipulations of expected testimony and
8 that work will require some time and because of that
9 and some other logistic issues to include some weather
10 issues that we're expecting tomorrow, this court is
11 going to go in recess tonight and we will begin again
12 like we did last week at 0930 on Monday morning.

13 Anything else that the parties would like
14 to add?

15 MR. FEIN: That was everything, ma'am.

16 MR. COOMBS: No.

17 THE COURT: Anything we need to address
18 before we recess?

19 Court is recessed 6:22 until 9:30 a.m.
20 Monday.

21 (Court adjourned at 6:22 p.m.)

	13:12;36:18	120:16;121:17;130:16;	65:19
A	accessing (2)	131:4,13,14;132:12;135:6;	admitted (4)
	35:12,13	147:13	19:3;29:20;30:11;66:4
Aberdeen (3)	accompany (1)	actually (29)	admitting (2)
66:13,16;93:15	101:21	9:6;13:5;19:16;20:1;	18:19;29:21
abide (1)	accomplish (2)	73:15;83:21;84:9;85:21;	adopted (1)
131:16	36:19,20	98:20;99:10;106:4;121:17;	37:14
abilities (3)	account (15)	131:2,12,18,20;132:3;	advancing (1)
68:20;81:8;95:14	18:4,13,14,15,17;20:21;	143:4;154:9;162:16,20;	51:7
ability (22)	45:2;114:7,10,14;115:14,	163:9;171:10;179:19;	advice (3)
2:10;25:11;45:10;48:7;	16;116:10;217:7;221:7	180:1;185:14;195:17;	55:20;56:14;72:3
62:12;109:18;124:17;	accountable (1)	198:11;200:21	advise (4)
140:19;172:3,5,7,20;173:2,	31:5	adapter (1)	70:17;71:11,14,19
13,14;185:16;213:6,8,13;	accounts (1)	195:5	advised (2)
214:1,4;217:21	116:8	add (15)	71:17;108:21
able (20)	Accreditation (4)	42:5;47:19,21;48:20;	affect (1)
15:18;17:1;81:9;86:14;	176:4,20;179:17;180:3	93:20;105:15;147:20;	51:1
88:4;97:15;106:5;118:6,9;	accredited (5)	158:8;162:20;163:16,19;	Afghanistan (1)
120:12;121:10;124:9,10;	28:16;33:13;42:6;175:18;	208:9,10;218:20;224:14	169:18
137:2;151:18;157:5;165:3;	179:19	added (4)	afternoon (7)
166:14;169:8;209:5	accrediting (1)	41:17;92:20;126:10;	19:10,11;21:14,15;52:5,
above (2)	42:14	147:16	6;83:11
70:14;109:12	accurate (1)	adding (8)	again (32)
above-titled (1)	2:11	43:14;154:9;157:20;	6:4;12:12;13:1;16:8;
1:15	ACCUSED (6)	163:2;165:2,4;208:3;	17:5;20:10;34:19;35:5;
absence (1)	3:10;65:7;108:3;132:2;	211:20	37:9;49:20;50:2;81:3;89:2;
113:11	186:4;223:16	addition (5)	91:6;97:21;101:18;108:20;
Absolutely (6)	achieve (2)	32:14;33:1;105:11;203:3;	123:4;130:14;133:19;
59:1,3;65:9;92:4;94:1;	72:1,10	208:13	135:5;136:14;140:17;
96:1	acknowledge (2)	additional (2)	148:9;194:13;196:13;
Academy (1)	30:20;34:7	33:2;150:16	201:1;205:19;211:5;
111:21	acquisition (9)	address (8)	221:13;224:3,11
ACAT (7)	69:3;70:7;71:7,13,19;	6:6;74:8;76:7;107:13;	against (3)
69:1;71:3;73:1;77:4;	72:9,19;83:20;84:8	133:9;170:20;224:7,17	71:8;75:15;87:21
83:19;84:12;88:8	acronym (2)	adjective (1)	agency (1)
accept (2)	67:15;118:15	71:1	22:12
75:21;105:14	across (11)	adjourned (1)	AGENT (10)
acceptable (14)	22:9,13;26:9;28:11;	224:21	4:4;7:3,5,11,13;10:13;
30:15,18,19;31:21;32:7;	56:10,11;68:20;69:21;73:2;	admin (13)	11:18;14:18;19:5,10
33:20;39:7;114:15;115:5;	82:9,9	97:4,4;100:13;102:6;	ago (3)
130:5,9;135:10;143:20;	act (3)	103:3;104:9;105:17;	148:4,7,21
164:2	77:4;113:12;160:3	154:16,20,21;155:16,19;	agree (4)
acceptance (1)	acting (1)	167:7	55:17;56:17;75:7;147:10
43:7	192:3	administer (2)	agreed (1)
accepting (1)	action (11)	42:11;162:19	160:4
210:10	27:8,10;29:10;33:19;	administrative (10)	agreement (4)
access (62)	43:12;44:15;46:20;57:4,5,	8:20;9:1;22:16;137:2;	32:12;34:2;107:12;
8:17,18;15:15,18;19:17;	7;72:7	140:12,18;141:11;142:20;	179:10
32:9,11,13;40:17;44:13,14,	actions (5)	155:3;217:3	ahead (13)
16;46:7,9,17;47:4,8;48:2;	34:15;58:4;64:1,6;160:8	administrator (25)	11:14;14:16;31:9;32:5;
54:8;60:8;80:7;95:20;	activists (2)	15:17;43:20;48:9;61:16;	35:4;38:17;41:9;109:5;
96:12;100:3,12,14;113:20;	53:11,12	62:11;63:14;140:13,14;	110:3;127:10;129:6;
114:1,4;119:12;139:11,18,	activities (6)	141:2;143:6;144:13,15,18;	185:10;219:3
20;155:9;165:13;166:5,7,7;	22:9;35:7;58:4;59:10;	145:7,9;173:3;197:9,10,15,	aid (1)
167:1;168:14,18,21;169:14;	71:2,18	17,20;201:3;208:14;217:6,	124:10
170:21;171:3,3,11,12,17,	activity (3)	16	air (4)
18;172:2,14,14,20;173:9,	11:2;45:21;63:8	administrators (10)	202:19,21;203:7,12
17;174:4,4,10,14,21;190:14	actors (1)	44:3;61:6;141:6,8,9;	Airborne (2)
accessed (2)	53:6	144:13,17;167:14;170:12;	112:20;180:19
64:7;103:7	acts (1)	217:15	alert (2)
accessibility (2)	77:3	admissible (1)	167:13,13
45:7;62:7	actual (14)	131:10	alerted (3)
accessible (2)	2:5;117:17;119:19,20,21;	admit (1)	159:4;182:12;184:4

ALEXANDER (1) 3:8	214:19	218:18,19;220:8	139:12;180:14,18;188:21; 189:6
algorithm (1) 8:7	ANGEL (1) 3:6	approve (1) 105:11	arriving (1) 123:20
allocated (1) 15:9	angles (1) 88:14	approved (15) 56:19;57:5;58:10,10; 64:16,20;91:11;95:2;142:8; 156:9,10;162:16;212:19; 220:2,3	ASHDEN (1) 3:4
allow (16) 41:20;44:2;46:6;52:11; 58:15,17;63:13;72:7;97:2; 102:16,19;143:4;167:15; 171:2,2;200:20	annual (2) 36:10;114:18	approximately (4) 12:8;27:16;28:2;111:16	aside (1) 59:11
allowed (12) 45:2;48:20;51:16;57:10; 96:19;121:15;169:16; 182:15;198:14;214:21; 215:5;219:19	annually (1) 36:13	AR (1) 34:13	assessment (1) 175:5
allowing (3) 127:8;161:3;173:15	anomalies (1) 51:14	AR25 (1) 26:14	assessments (1) 23:13
allows (9) 48:5,15;50:16;82:18; 106:9;107:16;140:15; 171:11,12	answered (1) 60:17	AR-25 (1) 130:8	assets (1) 171:16
all-source (1) 173:8	antisecurity (1) 55:11	AR25-2 (43) 27:2,4,15,20;28:6,7,12, 15,17;29:8;34:21;36:10; 45:18;51:2;54:16,17,21; 55:4,8,14,18;56:6,12,18,20; 58:17;63:4;115:9;117:3,17; 118:1,20;126:5,7,12,14,17, 20;130:6;134:9,11;143:16; 144:9	assignment (5) 21:19,21;22:1;112:7; 175:8
almost (1) 180:19	anymore (1) 49:19	Arabic (2) 74:21;86:12	assist (2) 7:15;42:6
Along (2) 81:14;147:6	apologize (1) 59:13	arbitrary (1) 58:6	assistant (1) 141:9
aloof (1) 177:20	appear (1) 182:16	area (4) 111:7;122:21;171:14; 174:19	associated (19) 16:3;18:8;22:15;24:7; 28:17;31:1;34:16;36:7; 44:13,15;50:16;58:5;59:10, 16;74:4;79:10,14;99:12; 101:13
alpha (12) 111:10,11;126:6;127:5, 12;128:8,11,20;147:9; 148:18;176:10,11	APPEARANCES (1) 3:1	areas (2) 24:6,7	assume (5) 53:21;56:7;64:9;162:14; 182:19
al-Qaeda (5) 53:1,16;54:1,11,14	appears (5) 10:17;18:12;109:17; 222:1;224:6	argue (1) 131:13	assuming (1) 114:7
alternate (1) 169:21	Apple (1) 10:5	argument (1) 183:13	assumption (4) 98:17;147:3;159:1,2
alternatives (1) 59:17	applicable (2) 28:14;39:16	ARMY (62) 1:2,7,9;22:2,3,4,7,9,13; 23:3;25:4;26:5,9,19,20,21; 27:18;28:9,11,19,21;29:13, 14;34:15;36:6,16;37:12,14; 40:9;55:9;56:11,16;61:17, 20;63:11;66:19;69:9,13,15; 70:1;71:6;72:11,21;73:3,11, 20;77:12;78:4,14,17,19,20; 79:1,10;84:13;85:17;87:12; 138:6;143:14;147:5;168:2; 184:2	assurance (36) 22:17,18,19;23:7,9,11,16; 24:4,6,14,18;25:5,20;26:2; 27:13;28:10;35:18,21;36:8, 13,15;39:4;40:5;113:13; 114:19;150:2,8,12,17; 153:1;159:21;176:3,17; 177:11,17;178:2
Although (5) 30:2;213:8;217:10,10; 219:17	applications (5) 45:9;46:15;48:7;106:11; 193:4	Army's (1) 26:7	attached (1) 62:20
always (8) 51:8;56:12;63:17;203:18; 207:1;218:19;220:16;223:7	applied (1) 151:2	around (7) 74:2;107:7;125:12; 150:21;157:17;188:19; 203:10	attack (1) 18:5
amazed (1) 191:17	applies (3) 28:13,14,20	arrival (2) 112:15;116:6	attacks (2) 17:18;40:16
amount (3) 131:2;151:20;207:5	apply (5) 20:11;28:9,12;102:12; 173:19	arrive (3) 112:10,18;188:18	attempt (1) 63:8
amusing (1) 118:15	appointed (1) 150:5	arrived (12) 112:12,13;115:21;116:3; 117:13;123:18;134:21;	attempting (1) 126:4
analogy (1) 182:17	appreciate (1) 221:13		attempts (1) 40:17
analysis (5) 43:6;71:15;75:8,9,10	approach (2) 22:20;76:6		attorneys (1) 108:19
analyst (5) 69:15,20;80:7;100:18; 194:20	approached (3) 192:2;197:1;208:20		attribute (1) 74:3
analysts (3) 173:8;190:6;213:18	Approaching (1) 115:20		attributes (1) 74:3
and/or (4) 44:14;48:16;59:13;	appropriate (7) 31:1;32:21;42:15;50:21; 51:15;57:4;164:20		audio (1) 2:8
	appropriately (1) 152:17		audio/video (1)
	approval (18) 48:9,10;93:7;161:4,10,13, 14,16,21;162:3,4,13; 163:17;211:21;213:6;		

2:8 August (1) 187:3 AUP (86) 32:21;115:2,4,8,15,18; 116:1,4,7,9,13,15,20;117:2, 3,4,8,9,14,16,17,21;118:1,3, 7,10,19;119:11,14,16,18,19, 20,21;120:11,13,16,18,19; 121:9,10,12,20,21;122:2; 124:10,11;125:9;126:8; 127:14,15;128:6,15,18; 129:5,11,13;130:16;131:3, 8,13;132:5,12;134:8,8,13, 17,21;135:1,5,6,19,20; 136:11,13;138:18,19; 145:14,18;146:4,8;147:4,7, 17,18;148:11 AUPs (13) 33:15;34:1,2;115:18; 117:9;122:11;123:11,15; 124:2,6;125:4;134:17; 138:21 Australia (2) 68:1,3 authenticity (1) 170:2 author (2) 27:2;28:4 authoring (1) 27:1 authorities (2) 42:10;51:11 authority (15) 42:5,8,14;55:20;56:3; 61:4,5;101:18;172:4,6,21; 173:6;175:1;210:13;216:18 authorization (19) 44:11;46:14;56:4;62:8,9, 13;83:3;147:21;148:9; 149:7,10;152:20;169:11; 173:14,16;174:18;213:9; 215:8;218:6 authorize (2) 32:20;156:17 authorized (52) 33:2;34:8,10;35:14; 42:11,15;45:20;46:18;55:6, 6;58:3;61:3;64:20;83:6; 94:5;97:1,2,4;101:3,5; 102:15,16;137:20;138:12; 141:14,21;142:4;143:11; 144:6;151:8;156:2;161:3; 185:1,5;195:12,15;198:7, 14,16;199:1;200:16,17; 201:7,9;208:6;209:3,8,9; 212:6;215:1;219:9;220:11 authorizing (1) 58:13 authorship (1) 28:1 automate (4) 47:19,21;48:2,8	automated (7) 47:11,13,16;48:6;69:1; 84:10;106:10 automates (1) 107:8 automation (2) 48:5;149:16 automations (3) 113:7;150:1;175:11 availability (2) 22:21;142:6 available (15) 87:15;88:2;90:4,6;92:12, 15;96:8;113:17;117:1; 123:10;142:2,3;151:13; 170:10;220:5 aware (12) 99:13;163:1,5,14;168:19; 173:7;175:16,20;177:2; 183:9,12;222:16 away (3) 189:16;212:2;213:16	84:2;85:18;104:10;121:9; 132:5;146:17;147:2; 169:11;171:21;183:3; 184:8;189:16;193:1; 205:14,19;206:1;210:19; 211:21;216:5,9;223:9 baseline (43) 55:14;76:12;78:1,2,9,11, 12,21;79:1;83:16;85:1; 91:10,11,12,19,21;92:10, 14;93:8,11,12,17;94:5;95:3, 7,9;98:18,19;101:9,13; 119:16;134:11;156:21; 163:20;209:1;210:5,12,12; 211:4,6,15;219:14;220:2 baselines (1) 77:21 basic (2) 68:16;111:7 basically (25) 9:18;13:11;25:15;34:2; 39:14;45:7;48:14,18;93:6; 109:13;147:1;151:11; 153:5;157:10;164:13; 173:8;175:10;176:6,15; 177:10,16;203:11;204:10; 217:9;221:10 basing (1) 146:12 basis (7) 36:11;48:4;146:1,2,9; 153:6;201:20 battalions (1) 70:12 batted (1) 157:16 battle (2) 69:18;217:7 battlefield (1) 145:1 BCD (1) 220:3 BCT (1) 149:16 became (3) 155:10;193:8;212:9 become (6) 68:17;83:16;84:21;111:9; 204:15,17 becoming (2) 68:14;91:11 began (4) 26:1,3,19;68:4 begin (5) 87:6,11;162:2,4;224:11 beginning (3) 202:16;217:4;221:4 BEHALF (2) 3:3,10 behavior (1) 31:6 behind (3) 95:20;201:19;203:10	belief (1) 216:20 below (1) 11:19 besides (1) 153:17 best (18) 23:17;28:2,4;72:9;88:1; 120:20;124:1,9;130:15; 135:7,8,10,18;136:11; 137:19;138:17;142:11; 147:4 better (2) 77:5;135:3 beyond (1) 163:20 big (3) 84:4;86:9;91:16 biggest (2) 84:5,13 bit (8) 45:15;52:20;73:6;95:21; 126:16;128:14;135:3;151:5 black (1) 109:12 block (1) 109:9 blow (3) 203:7,11,15 blows (1) 98:6 Board (1) 93:10 boards (1) 150:19 boilerplate (1) 118:12 bold (1) 86:15 bolded (1) 35:9 book (1) 210:9 boot (4) 9:4,20;13:7,10 bootable (3) 47:1,2,6 booted (3) 16:3,17,19 booting (2) 9:12;16:12 boots (1) 9:19 boss (1) 175:1 both (23) 7:17;15:7;18:15;36:4,16; 40:19;73:15;78:6;129:2; 182:14;186:9;204:1,13,14; 210:14;222:11,14,15,15,18, 19;223:3,5 bottle (2) 202:18;203:14
B			
bachelor's (1) 66:21 back (38) 9:9;16:5;19:7;63:10,21; 68:4;69:16;75:16;76:9; 80:16;82:3;86:2;97:17; 98:2,10;101:17;103:12; 110:4;117:11;123:18,20; 128:15;130:6;132:1; 146:17;158:6,8,14,15,19, 20;177:9;189:9;194:20; 195:2,7;209:7;220:1 backbone (2) 80:6,6 background (2) 66:20;181:6 backup (1) 2:9 backwards (1) 171:20 Bad (8) 8:9;41:5;53:7;61:9,9; 165:5,7;206:12 bandwidth (4) 79:16;80:2,10,13 banner (3) 32:10,14;33:4 bar (1) 170:20 barrel (1) 182:19 barring (1) 193:7 Base (3) 1:10;51:3;185:3 based (30) 12:6;15:12;31:15;36:17, 17;37:1;53:21;63:18;64:21;			

bottom (2) 39:12;165:1	built (3) 77:10,10,14	130:14;132:14,19;135:2,5,13;136:8;137:5;141:1;142:16,20;144:3;148:16;154:8;162:14,20;166:13;170:8,8,9;171:2;172:12,13;181:7;191:21;192:17;194:6,13;196:4;198:1;199:12;201:1;207:13,14;215:9;218:11,14,15,15;219:1;222:2,14;223:3	CD (32) 9:6,13,17,20;10:3;11:3;12:19;13:2,5,8,10;15:21;16:4,15,16,18;39:15;47:1,2,3,6;50:18;60:13;61:11;137:5;142:19;152:13,16;155:6,8,16;158:18
bought (1) 70:6	bulletin (7) 101:6;102:8,11,13;105:6;150:18,18		CDD (2) 73:14,15
boundaries (2) 35:14;53:17	burn (4) 9:15,16;12:4,21		CDs (12) 39:2,4,12,13,14,18,20;53:19;58:20;61:9;62:17;219:12
box (5) 46:8;63:14;82:12;103:3;109:8	burned (6) 10:3;11:3;13:5;16:14,16;124:4	cans (2) 203:7,12	center (2) 22:2,3
Bradley (1) 1:6	burning (4) 11:21;12:2,19;180:1	cap (1) 203:14	cert (2) 26:7,10
branch (4) 22:5,7;111:6,7	burrow (1) 86:11	capabilities (4) 46:16;69:12;71:16;73:12	certain (10) 75:19;94:13,18;99:1;167:1;171:7;200:4;210:9;214:16;218:18
brand (1) 26:7	business (8) 28:2,4;33:3;51:13;147:4;191:3,6;212:16	capability (6) 71:6,8;72:1;73:13;74:8;75:6	certainly (1) 71:7
break (3) 108:16;170:3;174:9	buying (1) 84:11	capable (1) 143:8	certificate (8) 24:19;25:11;37:2,4;138:1,4,5,9
breaks (1) 8:10	bypass (3) 45:21;46:3,11	capacity (3) 24:5;68:19;81:8	certificates (1) 112:2
brief (7) 38:18;108:17;123:1;133:2,16;164:17;224:1		caps (1) 202:18	certification (9) 24:15,17,21;25:8,9,10;112:6;176:3,20
briefing (1) 146:3	C	CAPTAIN (32) 3:5,6,7,8,12;5:4;21:2,2;32:15;108:15;110:14,17;111:6;120:15;123:15;124:16;129:19;132:4;133:13,20;134:7;135:13;136:8;138:13;139:6;145:13;156:2,9;160:20;172:17;178:15;183:9	certifications (2) 24:11;25:6
briefly (1) 224:5	C210 (1) 52:16	care (1) 189:20	Certified (5) 24:12,14;25:11;112:4;175:18
Brigade (48) 112:9,14,15;113:7,12,12;117:9;121:12,13;122:17;136:4;139:19;144:18;145:18;150:1,3,9,13,21;151:2;152:12;156:6,15;157:8;158:12,21;160:19;169:10;170:15,19,19;171:6,15;173:21;174:21;175:7,11;176:6,12,19;177:3,12;180:19;209:12,18;210:2,20;211:1	calendar (1) 166:15	career (3) 26:4;76:17;115:19	chain (7) 56:21;57:9,11;160:3;165:7,11;182:21
brigades (2) 70:14;171:14	Call (9) 6:8;72:17;73:12;77:11;88:21;89:6;110:5;162:3;207:3	carried (1) 219:12	chair (4) 109:7,11,13;133:21
brigade's (3) 113:11;149:15,19	called (22) 6:2,5;7:6;20:20;21:8;66:9;68:15;71:3,5;73:14;84:9;93:9;95:11;98:5;102:8;108:18;110:10;133:17;175:21;186:14;189:15;211:4	Carry (1) 185:20	change (9) 33:20;42:12;46:14,19;47:4;60:14;93:10;94:5;163:19
bring (4) 107:9;144:20;170:21;216:19	calling (1) 40:18	case (16) 16:9;18:3,7,10;92:9;108:2;121:15;131:5,5;133:14;155:11;157:5;164:10;186:3,4;223:16	changes (6) 42:9,10;136:6;140:20;141:5;216:18
brings (2) 107:10;194:15	Calls (6) 17:6;21:5;66:6;108:14;110:6;186:6	cases (4) 78:7;97:14;99:6;217:5	changing (1) 46:17
Bristow (1) 21:12	came (11) 67:10;68:4;128:15;160:19;164:11,12;209:19;212:9;220:1;222:1,7	catastrophic (1) 196:17	characterization (1) 118:17
broad (1) 53:15	Camp (10) 188:2,3,17;198:17,18,21;209:5;212:5;218:11;219:4	categories (2) 53:15;84:2	characterize (1) 72:16
broadly (1) 43:13	can (92) 8:4,10;9:2,7;11:5,18;12:13,14;13:20;14:18;34:8;39:5;42:17;44:8;46:7;47:11,13,19,21;49:7,13;53:8;59:14;63:2;76:13;77:5;80:5,20;81:18,20;82:10;86:7;87:15;92:19;93:8;95:14,19;100:16;103:20;104:6,6;110:3;111:17;117:16;119:6;121:12;122:4,7;127:12;	category (2) 69:2;83:20	characters (2) 15:13;86:8
broken (2) 8:14;111:19		caused (1) 193:3	charge (7) 71:2;121:4,6;146:3;150:7,11;157:10
brought (1) 119:6		causing (2) 196:8;206:21	charged (3) 31:16;34:20;50:2
build (12) 18:16;73:16,20;74:1,7,18;75:3;85:18,21;87:6;91:3;119:16		cave (1) 193:14	Charles (1) 70:18
building (4) 79:10;81:4;89:5;91:4		caves (1) 204:11	

Charlie (1) 176:10	22:6;34:11;208:13	2:18	138:18
Charlottesville (1) 186:19	clarification (1) 129:9	Colonel (7) 1:18;156:5,5,8,16; 157:19;209:15	compared (1) 135:6
charter (1) 87:5	clarify (1) 132:13	combinations (1) 2:17	compares (2) 117:17;130:15
chartered (1) 70:21	classified (15) 40:8;50:19;53:18;54:9; 109:15,17;113:17;118:14, 16;130:12;151:21;152:6, 13;180:1,6	COMBS (2) 120:10;128:8	compartmentalized (2) 166:2,3
charts (1) 71:5	clearance (3) 114:5;169:1;179:9	coming (8) 132:11;201:6;205:1,3,7, 20;206:5;216:18	compatible (1) 218:8
chat (43) 14:10;19:13,21;41:19; 101:3,11,19;102:21;104:17; 105:12,16;106:7,8,12,21, 21;107:2,14;153:20;154:4; 156:10,17,20;157:20; 209:19;210:4,11,16,17; 211:3,7,12,20;212:3,13,17; 218:3,4,13;219:8,15,18; 221:19	cleared (1) 50:20	Command (24) 22:8;26:13;33:11;56:21; 57:3,9,11;74:12;77:13; 93:14;110:20;145:1,1; 147:16;159:4;160:3,4; 165:8,11;182:8,12,21; 183:19;184:6	complain (2) 205:3,8
chats (1) 15:13	clearly (1) 42:4	commander (29) 42:19;44:3,9;55:17,19; 56:13,14,18;58:3,13;59:6; 101:8,15,18;102:3,17,18; 104:21;105:2,11,13;156:6; 157:8;209:12,17,19;210:2, 20;211:2	complained (1) 205:10
check (3) 94:3;141:21;142:8	click (7) 64:3;106:11;107:10,15; 163:9;182:3;213:4	commanders (6) 28:15;44:20;101:11; 102:14;104:16,20	complaining (1) 205:2
checklists (2) 23:17;82:8	clicked (1) 154:14	commander's (2) 101:15,17	complete (7) 12:4;36:14,15;38:12; 114:8,19;127:1
checks (1) 17:19	clicking (2) 63:18;64:19	commands (1) 155:4	completed (4) 12:21;38:1,6,8
CHEREPKO (23) 5:4;108:15;110:7,9,14, 17;111:6;123:15;124:16; 129:19;132:4;133:13; 134:7;135:13;136:8; 138:13;139:6;145:13; 156:2,9;160:20;178:15; 183:9	clicks (1) 63:3	comment (1) 191:15	completely (2) 123:10;170:11
Cherepko's (1) 172:18	client (8) 82:11;100:7,9,13,16,19; 129:11;131:6	comments (2) 191:4,14	Completion (2) 37:5;77:14
Chief (3) 6:14,16;22:4	client's (1) 124:17	commercial (2) 41:19;96:8	complex (1) 172:10
Chinese (2) 74:21;86:7	clip (2) 62:21;63:3	commercially (1) 87:15	compliance (7) 22:5,6,7,9,12;23:11;42:13
choice (1) 210:13	clips (1) 180:20	commissioner (1) 33:11	complicated (1) 13:20
chose (2) 101:8;215:16	closed (1) 128:19	common (10) 15:21;66:19;72:10;80:17; 99:14,18;209:16;210:17; 213:2;216:13	comply (2) 30:20;157:5
chunks (2) 75:1,2	closely (1) 171:7	communication (5) 67:3,15,18;113:5;211:7	compression (2) 209:1;221:5
CIOG6 (2) 26:19,21	Closing (1) 12:3	communications (6) 70:4;80:5,6;93:14;111:1; 149:20	compromised (1) 64:6
CIO's (1) 24:4	CNN (2) 118:15,15	communities (1) 80:13	computer (106) 8:3,5,15,18;9:13,18;13:8; 14:13;15:8,11;16:9,16;18:6, 18;22:14;24:6;26:5,8,20; 36:17;37:1;43:10;46:7; 47:12,16;61:20,21;63:20; 102:20;103:1,21;140:8; 141:18;142:13;143:9,12; 151:17;154:9,13;155:19; 160:21;163:3;167:5,11,18; 169:1;170:5;172:13; 178:17;191:1,3,5,13,15,19; 192:3,7,10,12,15;194:10,15, 18;195:2,13,17,20;196:14, 19;198:12;199:8,11;201:12, 18;202:11;203:19;205:2,4, 8,16,21;206:8,13,19;208:3, 10,17;211:3,17,20;212:13, 14,18;214:20;215:7,9; 216:2,12;217:13,20;218:3; 220:6,10,19;221:5;222:8
circumvent (10) 45:21;47:9;64:1;136:7; 143:4;154:20;174:13,15; 200:21;201:3	code (4) 34:18;64:3;77:11;147:20	community (4) 28:20;68:5;71:10;75:20	computers (30) 15:7;16:3;102:1;144:21; 156:17;157:2,20;167:9,17; 175:17;191:16;195:10; 202:15;203:5,11,13,17,21; 207:18,20;208:14;209:20;
circumventing (1) 154:21	coding (1) 46:14	companies (1) 70:12	
CIS (2) 110:19,21	coerce (1) 46:19	Company (4) 1:8;69:6;70:11;174:2	
CISSP (2) 24:15;112:4	Cole (1) 70:18	comparatively (1) 96:11	
civilian (3)	collaboration (4) 27:3;210:16;211:9,12	compare (4) 128:21;135:19;136:12;	
	collaborative (1) 211:7		
	collected (1) 122:15		
	College (3) 67:1,11,12		
	colloquy (1)		

210:3;213:11,12;214:13; 215:21;216:7;217:10,11	consistent (1) 61:17	185:9,20;186:10;192:4; 202:5,6;223:10;224:16	180:10,11;183:3,7;185:10, 18,21;186:2,8,11;192:9; 194:14;202:4;221:15,17,18; 223:9,12,14,20,20;224:2,3, 4,10,17,19,21
concept (1) 23:5	consolidated (1) 30:3	copied (1) 158:17	COURT-MARTIAL (1) 1:6
concerned (3) 82:13;99:3,4	constant (1) 89:10	copper (1) 184:3	courtroom (1) 2:6
concert (1) 56:13	consumption (1) 174:20	copy (1) 39:19	co-user (1) 192:1
conditioned (1) 202:21	contact (4) 198:13,17;200:21;209:4	copying (3) 48:18;60:8;158:18	cover (2) 40:5;222:11
conduct (6) 22:13;31:5;33:3;45:21; 51:4;60:15	Contacted (1) 212:5	copyright (2) 58:18;59:11	covered (3) 35:8;115:8;134:13
conducted (1) 55:10	contain (6) 2:14;61:10;63:6,19; 181:9;219:6	core (4) 56:15;68:6;70:13,14	covering (1) 109:12
conducting (1) 36:13	contained (4) 11:19;17:4;19:17;120:18	corner (1) 39:12	covers (2) 40:6;135:9
conducts (1) 89:1	contains (1) 7:17	Corp (1) 171:15	CPD (4) 73:13,17;74:2;85:17
conduit (1) 77:4	content (21) 35:15,16;36:6;41:5;42:6; 48:3,16;61:10;63:6,19; 64:7;117:20;118:3,4; 120:18;130:18;135:8,11; 147:8,13,14	Corps (1) 28:20	CPT (1) 36:17
confident (1) 107:1	contents (11) 9:8;13:6,17,21;17:1,3; 38:7;39:13,14;116:19; 130:10	correctly (4) 59:9;62:1;201:4;219:21	crack (3) 18:6;216:11;217:6
confidentiality (1) 22:20	context (1) 13:15	corrupt (9) 193:7,8,17;194:6;204:1,6, 15,17,20	cracking (2) 17:21;221:6
configurable (1) 41:18	continue (2) 62:5;105:4	cost (8) 75:15;76:12;79:9,14; 88:1,3;90:6;101:13	craft (1) 47:17
configuration (1) 60:15	continued (12) 1:16;4:5;5:1,13,14,15; 7:10;19:9;182:15;183:8; 184:10;185:12	counsel (3) 119:5;186:4;223:16	crafted (1) 47:3
configurations (2) 107:13;157:4	contract (2) 24:2;87:13	counterintelligence (1) 71:5	crash (5) 193:14,15;196:9;203:15; 207:7
configure (3) 9:5;107:17;195:1	contractor (6) 26:6;97:8;187:13,14,17; 188:10	couple (11) 10:16;46:10;61:14;83:18; 100:21;104:13;180:10; 184:8;191:14;217:5;221:17	crashed (3) 151:17;206:8,13
configured (6) 45:8;62:1;167:9;169:16, 21;171:1	contracts (1) 77:9	course (6) 28:2;111:11,12,19; 115:19;116:12	crated (1) 135:1
confirm (1) 222:14	contributed (2) 36:6;193:5	courses (1) 72:7	create (13) 17:16;45:10,11;87:4; 90:6;96:16;117:4;118:11; 119:20;126:7;147:4,7; 194:8
confused (1) 123:10	control (8) 2:10;35:14;46:17;59:15; 64:15;145:2;167:16;197:21	court (152) 2:3,14;4:17;5:12,20;6:2, 2,3,4,4,8;11:14;14:16;17:8, 10;19:2,6,8;20:6,8,10,16,16, 19,19;29:3,18;30:4,4,7,9; 31:9,19;32:1,4,15,18;35:1, 4;37:19;38:3,9,14,17,21; 41:1,9;49:2,7,16;50:3,8,12, 14;51:21;52:2;59:20;61:14, 15;64:21;65:3,5;66:1,3; 83:9;95:16;100:21;101:2; 104:10;105:4,9;106:18; 107:19,21;108:7,18,18,19, 20;109:1,5,10,11,17,21; 110:3;111:17;112:8;119:9; 120:15,20;121:14;122:2,6, 9;123:9;124:12;127:8; 128:11,21,21;129:2,12; 130:14;131:17;132:7,16,19; 133:3,8,11,13,17,17,18,19; 134:3,5,16;135:2;148:17; 149:13;176:9;178:13;	creates (1) 8:7
confusion (1) 131:14	controlled (1) 33:6		creating (3) 27:3,17;147:16
Congress (2) 71:21;84:1	controls (5) 47:5,10;165:13;168:14, 18		creation (1) 61:2
connect (6) 80:20;81:10,12,18; 107:14;195:3	conversation (1) 223:4		creative (4) 73:6;202:17;203:1,14
connected (3) 96:5,6,10	COOMBS (32) 3:11;6:9;66:2;108:16; 109:20;119:3,10;121:1; 124:14,15;129:3,9;130:21; 133:7;134:14;145:12; 149:12,14;176:10;178:11; 180:9;183:4;184:8,10;		criminal (1) 121:9
connections (1) 171:10			critical (6) 76:9,10;79:12;81:11,16; 88:10
connectivity (2) 96:3,12			CROSS (7) 4:9,15;5:10,19;52:2; 53:17;179:16
connects (1) 81:13			Cross-examination (9)
cons (1) 56:6			
consider (3) 56:5;72:3;181:1			
considered (1) 62:21			
consisted (2) 111:18;132:6			

19:6;49:8;52:4;83:9,10; 129:3;145:12;202:4,6 current (9) 24:1;27:11;53:4;68:11; 70:17;72:12;93:17;110:17; 186:21 currently (3) 24:12;27:10;68:18 cursor (1) 82:16 customer (1) 191:10 cyb (4) 211:4,8,9,13 Cyber (5) 22:7,15;26:13;81:21;82:1 cycle (1) 91:20	dates (1) 12:8 DAVID (4) 3:11;4:4;7:3,5 dawgnetwork (1) 14:21 day (11) 164:7;179:4,5,12;180:18; 192:2;205:6;220:4;222:5, 12,13 days (1) 164:16 DB (1) 171:14 deactivated (1) 115:14 deal (1) 94:10 dealing (1) 56:11 December (1) 92:6 decided (1) 94:2 decides (1) 33:13 decision (7) 23:16;56:1;72:8;76:6,11; 77:8;166:19 decisions (2) 55:5;56:14 decompensation (1) 85:15 decomposed (1) 75:1 decrypt (1) 18:2 decrypting (1) 17:21 dedicated (1) 27:17 defense (29) 22:14;24:3,3,7;26:12; 30:7;31:15;34:19;36:12; 37:20;68:2;69:3;77:3;84:1; 119:3;126:5;127:5,11; 128:10,11,20;130:21;132:9; 147:9;148:18;176:3; 179:16;183:4;186:10 Defense's (1) 131:19 defiled (1) 115:13 defined (5) 73:2,12;92:10;93:9,13 defines (4) 44:10;78:21,21;91:12 defining (1) 73:10 degree (2) 66:21;67:1 delegated (2) 146:6;178:18	delete (2) 194:7;207:14 deleted (3) 158:5,14;164:15 delicacy (1) 217:14 delineate (1) 75:4 deliver (2) 75:5;219:5 delivering (2) 79:15;81:6 delivers (1) 80:17 Dell (1) 9:19 Delta (1) 176:10 demeanor (1) 46:21 Denise (1) 1:18 Department (6) 24:3;26:12;36:12;61:20; 84:1;176:2 depending (2) 89:4;99:7 depends (2) 47:3;161:2 deploy (2) 112:16,21 deployed (12) 80:12;92:2;94:10;97:7; 112:15;117:11;131:16; 146:13;150:17;176:20; 187:14;212:1 deploying (1) 112:14 deployment (14) 123:2;127:18,20;131:21; 187:16,19;188:1,9,12,15; 196:19,20;197:4;212:1 deploys (2) 92:5;97:17 describe (1) 111:17 described (2) 58:14;212:4 description (2) 25:7;73:13 descriptive (1) 41:21 desert (1) 203:4 design (15) 28:18;46:2;76:4,9,10; 88:9,10,11;89:14,16;90:10, 16,17,19;95:21 designating (2) 28:16;42:14 designed (7) 45:13;53:19;80:1;95:18; 155:1;176:16,16	designing (1) 91:3 desk (10) 114:6;122:12,17,21; 141:20,21;142:4;144:19; 146:6;185:17 desktop (30) 105:16;137:7;142:19; 143:7;144:21;154:13; 155:6,18;163:3;167:5,11; 185:15;193:11,15;201:5; 204:3,5,14;206:20;207:1,4; 213:4,14,17,21;214:1,4,8,9; 222:3 desktops (1) 202:18 destroyed (2) 123:8;124:8 detail (1) 73:17 detained (1) 124:20 determination (3) 44:9;177:4,7 determine (2) 44:4;208:18 determined (6) 33:8,10;42:15;194:18; 198:21;212:6 determines (3) 33:13;44:18;84:4 determining (2) 71:15;79:17 develop (1) 72:17 developer (2) 85:20,21 developing (2) 37:16;72:6 development (9) 72:15;77:12,15;84:4,8; 86:3,20;87:14;91:2 deviate (1) 55:18 deviated (1) 56:6 deviation (2) 56:17,18 device (1) 152:3 DIACAPP (5) 175:21;176:7,13,15; 177:9 diagnosis (1) 206:2 dictate (2) 44:1,2 dictionary (1) 17:18 difference (3) 60:2;104:2;128:14 different (15) 40:10;47:6;75:4;81:13,
D			
D6 (18) 76:18;145:3,5,7;190:4,8, 11,14;195:12;197:10,10,20; 198:8,11;199:11;200:14,18; 201:15 D6-A (79) 68:4,8,20;69:10,11,15; 70:1,6,9,12,16,18;71:3; 73:14,16;80:17;81:13;82:3; 83:6;85:17;89:4;91:18; 96:2,4,19;97:8,18;98:3,11, 13,16;99:14;102:1,3,20; 103:20;156:17,21;157:1,3, 20;167:16;188:6;190:1; 202:11,14,20;203:4,17,19, 21;208:3,10,14,17,21; 209:20;210:3,12,15,17; 211:3,10,17;212:10;213:10, 12;214:12,20;215:6,21; 216:7,11,19;217:2,15; 219:5,14;220:19 DAA (3) 42:14;44:4;48:9 daily (5) 44:17;146:1,2,9;201:19 dash (2) 12:1,19 data (21) 12:2;69:17,17;70:3; 96:10;98:21;99:5;137:16; 190:6;193:14;194:7;195:5; 206:16;207:5;222:18,19; 223:2,3,5,6,8 database (1) 13:19 databases (1) 96:13 date (1) 125:1 dated (5) 6:19;27:14;29:10;65:15; 108:10			

15;84:7,9;88:14;94:19; 95:21;133:1;157:8;189:15; 218:13;219:18 differently (1) 60:19 difficult (2) 70:2;167:2 digital (2) 40:18;149:19 digitally (1) 37:2 DIRE (8) 5:6,8;119:6,9,10;124:12, 15;127:7 DIRECT (17) 4:8,14;5:5,7,9,18;7:10; 21:11;28:1;83:14;99:16; 110:13;122:10;129:16; 186:17;208:5;209:6 directions (1) 52:12 directives (1) 27:18 directly (5) 22:3;67:10;68:6;211:1; 222:2 director (2) 68:18;71:14 DIS (1) 26:12 disagree (2) 55:8;177:6 disagreed (1) 177:3 disappear (1) 164:14 discharge (1) 182:18 discipline (3) 177:11,16;178:1 disciplined (1) 176:17 disciplines (1) 23:6 DISCLAIMER (1) 2:1 discrete (1) 89:6 discuss (7) 38:7;54:5;65:6;108:1; 133:14;186:3;223:15 discussed (4) 52:21;53:1,4;62:16 discussing (1) 35:1 discussion (1) 32:2 disk (6) 10:7,17,19;12:6;13:5; 143:7 display (1) 32:11 displayed (1)	139:2 disposition (1) 99:11 dissemination (1) 69:13 distance (1) 169:21 Distributed (2) 66:19;70:9 distribution (1) 9:15 dive (1) 193:4 division (6) 22:7;34:20;52:16;70:12; 162:3;210:14 divisions (2) 126:13,15 doctrine (1) 74:12 document (24) 10:14;13:18;29:7;73:13, 14;85:1,4,6;115:5;118:18; 121:17;127:1;129:20; 130:2,4;131:20;132:1,2,10; 143:17;146:12;147:7; 163:18;166:16 documents (9) 27:20;61:2;114:12;123:2, 11;172:8,18;181:20;207:6 DoD (18) 24:4,18;26:12;27:18; 30:20;33:20;35:17;36:11, 16;37:13,13,14,18;38:1; 39:3,4,5;84:11 domain (19) 55:11;139:20,21;151:14; 169:12,12;170:5,7,18; 171:11,12,18;172:13; 173:15;174:6,6,7,11,14 done (18) 43:7,7;56:12;59:9;67:8; 91:9;94:12;98:12;150:12; 156:13;160:2,6;161:1; 162:17;165:10;178:6; 198:20;202:2 dope (1) 126:2 dot (11) 12:1,20;13:1;14:13;15:5, 5,10,10;184:16,16,16 double (5) 64:19;107:10;154:13; 182:3;213:4 Doug (2) 65:15,17 down (10) 12:14;72:5,6;82:18; 86:11;88:19;111:19;128:4; 170:3;222:17 download (8) 9:14,16;48:15;95:15; 104:7;106:8;107:9;144:3	downloadable (1) 39:4 downloaded (1) 222:2 downloading (4) 35:11,12;48:16;60:13 draft (3) 2:13;117:9;134:20 drafted (1) 27:21 drafting (2) 27:15,17 drastic (1) 196:6 draw (1) 124:10 drive (41) 13:12;48:19;60:9,9; 103:6,11,11,12,16;137:5,6; 139:10,21;141:7,8;142:19; 151:6,16,18;155:8;165:14; 169:14,19;193:3,19,19; 194:1,2,2,21;195:1,4,4,5,6, 7;196:8,10;207:8,10;222:20 drives (3) 150:20;194:19;197:5 Drum (12) 112:10;115:21;122:2; 123:19,21;124:6;127:14,21; 128:15;129:5;132:1;189:9 due (4) 2:18;57:3;58:18;202:11 duly (5) 7:6;21:8;66:9;110:10; 186:14 during (8) 109:4;112:3;116:12; 131:21;133:14;187:21; 188:14;196:19 dust (5) 98:6;203:3,8,11,15 dutiable (1) 60:14 duties (3) 22:16;26:21;34:7 duty (8) 21:19,20;22:1;44:12; 149:18;150:5;175:8,13	easy (2) 36:18;172:11 ECAT (2) 71:4,4 ECRB (2) 93:10,10 edit (5) 140:2;166:16,17;172:7, 18 editing (2) 2:9,16 editor (4) 13:14,16,20;17:1 educate (1) 217:18 educated (1) 147:1 educating (1) 217:9 educational (1) 66:20 effect (1) 47:1 effective (1) 77:19 effects (1) 47:2 effort (2) 27:17;48:17 efforts (1) 28:9 Either (8) 28:3;54:2;64:16;76:5; 142:2;181:18;191:2;209:5 elect (1) 92:11 electrical (2) 67:1,2 Electronic (2) 66:18;187:10 electronics (1) 93:14 element (1) 38:10 elements (1) 70:14 elevate (3) 46:6,16;202:18 elevated (2) 47:5;140:14 elicit (2) 121:19;192:6 eliminate (1) 88:20 eliminated (1) 124:16 eliminating (1) 213:21 else (8) 22:10;41:21;123:12; 191:12;195:11;206:11; 218:8;224:13 Elten (47)
		E	
		earlier (8) 74:5;134:7;142:15; 144:12;182:4;183:11; 201:14;212:4 Early (2) 12:9;221:9 earn (1) 37:4 Earth (1) 198:3 easily (2) 8:10;54:9	

3:8;21:3,4,11;29:1,4,16; 30:12,14;31:7,10,20;32:3,6, 15,17,19;35:2;38:4,11,16, 19;39:1;40:1,3,21;41:2,10; 49:9,17;50:4,10,13;51:20; 60:1;61:12;65:1,4;66:5,12; 83:7;99:21;100:20;104:12; 106:2;107:18,20 e-mail (5) 34:11;40:11,18;62:20; 63:19 embedded (1) 97:8 emergency (2) 26:8,20 employ (1) 168:13 employed (2) 67:12;192:21 employee (2) 67:6;68:6 empowered (1) 74:6 enabled (1) 80:9 enables (1) 80:6 enabling (1) 46:18 EnCase (1) 14:12 encompasses (1) 60:5 encountered (1) 205:14 encrypt (2) 165:17,20 encrypted (4) 7:17,20;8:2;165:15 encryption (1) 174:9 end (5) 37:2,7;69:17;124:21; 184:15 ends (2) 90:16;109:13 enforced (1) 58:11 enforcing (1) 182:8 engage (1) 90:3 engaging (1) 77:2 engineer (12) 67:16;68:14;76:19,19; 97:13;100:3;102:4,5,11; 111:8;188:8;209:5 engineering (10) 67:1,2,21;72:20;75:17, 20;89:1,7;93:10,18 Engineers (6) 28:20;74:12;101:7,10,21;	104:21 English (2) 74:20;86:12 enough (1) 20:1 ensure (8) 23:2;56:9;93:16;109:15; 176:16;177:10,16;178:1 ensuring (3) 73:19;150:8,11 entail (1) 22:10 enterprise (3) 56:10;111:20;144:21 entire (7) 15:8;48:16;70:1;79:7; 95:15;98:20;189:11 Entirely (2) 100:6;217:13 entities (1) 89:6 entrusted (1) 51:10 environment (5) 58:6;80:12;177:17;178:2; 202:11 environments (1) 41:20 equal (1) 62:13 equate (2) 48:6;62:7 equipment (4) 70:11;78:8;109:1;110:1 equipped (1) 70:15 escapes (1) 67:15 especially (1) 121:1 ESPNcom (1) 54:14 essential (2) 157:2;160:20 essentially (30) 69:11;72:6,20;73:16; 74:14;75:1,12;77:9,17;78:2, 9,15;79:9;80:7;82:3,17; 83:1,21;87:4;91:3;93:11; 95:13,18;98:20;101:10,12; 103:7;107:7,15;217:8 establish (4) 26:8;31:20;44:20,21 established (4) 167:7;169:20;171:7,13 establishes (2) 28:7;31:21 Establishing (1) 35:2 evaluate (3) 74:13,14;77:13 evaluated (1) 23:14	evaluates (1) 77:13 evaluation (2) 75:15,15 even (13) 86:11;125:19;131:7; 146:8;147:18;158:5; 161:19;164:10;174:21; 201:6;202:20;215:4;217:19 event (1) 25:14 events (3) 25:17;168:3;210:7 eventually (3) 27:4;193:13,15 everybody (2) 28:13,21 everyone (11) 115:17;119:11,14,18; 120:3;150:16;158:5; 163:18;166:16;179:8,14 evidence (6) 10:5;18:20;38:5;120:20; 125:21;131:5 exact (2) 53:13;125:1 Exactly (4) 86:16,18;193:21;211:14 exam (1) 195:21 EXAMINATION (40) 4:8,9,10,11,14,15,16,17, 18,19;5:5,7,9,10,11,12,18, 19,20;7:10;21:11;60:1; 61:15;66:12;99:21;101:2; 104:14;106:2;110:13; 119:10;122:10;124:15; 129:16;178:14;180:11; 183:8;184:10;185:12; 186:17;221:18 examined (6) 7:8;15:7;21:10;66:11; 110:12;186:16 example (25) 9:20;11:9;48:2,4;50:7; 53:16;60:9;61:11;63:21; 74:17;75:18;85:5;87:9; 88:7;101:19;104:6;118:12; 147:5;166:13;173:2; 174:19;184:1;200:11; 204:7;212:21 examples (4) 34:18;35:6,6;42:1 exceed (2) 51:11,11 Excel (3) 45:11;48:2;181:20 exception (4) 21:2;33:5;114:20;115:2 exceptions (1) 56:12 exchange (1) 68:1	excusal (4) 20:8;65:3;107:19;185:21 excuse (1) 124:6 excused (5) 20:11;65:5;108:1;186:2; 223:14 EXE (1) 184:16 executable (68) 52:7,11,17;59:2;60:10; 61:5;62:9;63:1;105:16; 136:18,21;137:1,8,15,20; 143:1,3,9,15,18;153:14,17; 154:2,5,7,12,20;155:6,13; 156:3;158:2;163:1,2,6,8,16; 164:4;167:5,11,14,18; 168:10;181:5,19;182:2; 183:16;184:11,17;199:13, 16,17,21;200:8,9,13,17,20; 201:2,5,9;213:1,3,13,21; 214:9,19;216:7;221:19 executables (2) 61:8,10 execute (7) 52:13;56:2;60:11;63:20; 64:4,11;76:13 executed (1) 64:19 executes (2) 79:12;155:4 Executive (1) 66:17 exercises (1) 111:4 exhausting (1) 194:17 Exhibit (56) 6:11,12,13,15,20;10:8,10; 11:17;12:11;14:1,4;18:20, 21;19:2,7;29:2,17;30:11; 38:20;41:1,11;51:21;65:13, 16,20,21;66:3;108:8,11; 119:1,4;126:6;127:5,12; 128:8,11,20;129:1,7,17; 130:20,20;131:19;132:18, 19;133:5,5;134:2,5;135:14; 139:4;147:9;148:18,18,19; 149:12 exist (4) 123:16,18;125:11;167:12 existed (2) 124:11;125:4 expect (2) 57:10;82:10 expectation (1) 33:4 expected (4) 65:14;108:6,9;224:7 expecting (1) 224:10 experience (10) 21:16;56:8;72:5;90:15;
---	--	---	--

<p>92:15;196:12;203:18; 216:9;218:17;220:12 experiences (1) 56:11 expert (2) 24:5;221:20 expertise (1) 25:3 experts (1) 74:10 explain (16) 7:21,21;11:18;12:12; 16:12;70:2;117:16;130:14; 135:5;140:17;142:16; 165:5,6;191:21;194:13; 196:4 explained (2) 159:18;193:11 exploit (1) 190:7 exploration (1) 69:13 explore (1) 49:5 export (1) 82:18 extent (2) 49:6;53:8 external (1) 86:3 extraction (1) 48:3 extractor (1) 169:16 extremely (1) 53:18</p>	<p>123:6;130:2;136:18; 137:10;12;138:1;139:6; 142:15;145:3,4;155:11; 184:18;199:3,13,20;209:15 familiarity (1) 49:6 far (6) 127:21;132:8;171:12; 175:7;213:6;223:3 faster (2) 18:2;20:14 feasible (2) 47:8;59:12 feature (2) 8:8,13 features (1) 88:4 February (3) 11:20;127:16;187:20 feed (2) 2:8;69:20 feedback (1) 89:10 feel (4) 179:11;215:5;218:14,15 FEIN (23) 3:4;6:7,10,18;20:13;21:1; 30:1;65:11,19;108:5,8; 109:3,8;110:2;122:4; 123:13,14;124:5;127:7; 133:2,12;223:18;224:15 few (14) 35:6,6;112:15;115:9; 122:7;140:1;148:4,7,21; 170:13;191:4;197:1;202:9; 208:2 fiber (1) 184:2 field (13) 26:4;69:7;78:3;92:17,20; 97:13;100:2;101:7,18; 102:11;104:20;188:8;209:4 fielded (1) 69:6 fielding (1) 78:7 fighter (2) 72:2;79:3 fighter's (1) 79:2 file (94) 7:13,16;8:11,12,19,19; 9:3,7,16;10:7,18,20;11:21; 12:2;13:2,9,14,19,19,20; 14:13;15:4,8,10,15;16:21; 17:3;18:2,9;19:19;52:8,11, 13;60:4,4,5,6,7,10,14;61:1, 2;63:1,6;64:10,17;104:5,7; 105:16;106:9;107:9,15; 136:19,21;137:1,8,15,20; 143:1,3,9;154:2,5,7,12; 155:1,6,13;163:1,8;165:18, 21;166:11;167:11;168:10;</p>	<p>173:4;182:2;199:14,16,17, 21;200:8,9,12,13,20;201:2, 5,9;213:1,3,13,21;221:19 files (45) 8:16,16;35:16;45:10; 48:15;52:18;59:2;61:5,11; 95:19,20;96:1;99:15; 139:11;140:2;143:15,19; 153:14,17;154:21;156:3; 158:2,6;163:2,6,16;164:5; 165:14,17;167:5,14,19; 181:1,19;182:2;183:16; 184:11,15,17;199:18;200:7, 17;214:9,20;216:7 filing (1) 28:15 fill (4) 114:13,14;140:7;198:19 filled (2) 44:5;114:2 final (1) 90:19 finally (4) 8:15;12:4;17:13;189:8 find (26) 10:1;15:9,16;46:15;85:8; 92:9,15;116:16,17;125:17, 19;161:11;163:5;164:4,5,8; 173:21;175:2;180:20; 183:15;184:20;185:5; 201:20;207:12;209:7; 222:19 fine (3) 148:8;183:7;186:10 finish (2) 91:3,4 finished (2) 129:20;188:17 firing (1) 182:19 first (33) 6:13;8:8;9:10,14;11:9; 14:10;21:8;27:12;66:9; 73:10,18;85:11;90:13; 93:12;110:10;112:7;114:3; 157:9,13;165:6;175:8,11, 13;186:14;187:16;192:2; 193:2;197:1;205:5,11; 209:3;212:1,2 fits (2) 85:9;87:20 five (3) 26:9;68:9;197:6 fix (3) 191:10;206:7;207:12 flash (2) 137:5;155:8 Florinda (2) 108:9,12 flow (1) 202:19 fly (3) 189:16,20;212:2</p>	<p>flyers (1) 150:18 flying (1) 69:18 FOB (49) 112:17,18,21;113:3,6,18; 116:3,6;117:13,17;122:11; 123:11,15;124:2,7;126:1; 130:16;132:6,15;134:8,18, 21;135:6,19;136:12;137:9, 11,19;138:8,18;139:7,12; 142:11;145:16;176:19; 188:16,18,21;189:5,13,16, 18;190:12,17;191:19;199:3, 6,10;201:8 FOB's (1) 184:1 focus (2) 67:3;89:5 folder (11) 122:16;123:3;156:3,9; 166:5,12;172:18;173:21; 180:19;194:7;207:6 folders (1) 166:4 folks (2) 59:14;210:10 follow (5) 25:16;28:16;50:6;136:5; 215:16 followed (4) 57:3;58:11,12;150:9 following (1) 220:4 follows (6) 7:9;21:10;66:11;71:7; 110:12;186:16 followup (2) 183:3;223:9 follow-up (1) 104:10 Force (1) 110:20 foreign (4) 53:3,6,9,12 form (4) 114:6;198:20;210:3,6 formal (1) 151:1 formalizing (1) 26:7 format (3) 29:13,15;39:15 formats (1) 82:19 formed (1) 22:8 forms (1) 114:2 Fort (2) 1:11,17 forth (7) 23:17;28:20;40:12;45:11;</p>
F			
<p>F9 (1) 9:20 facets (2) 23:5;79:12 fact (4) 58:18;131:11;160:13; 214:12 factors (1) 40:16 failed (1) 206:3 fails (1) 196:10 failure (2) 35:14;196:17 failures (1) 196:5 fair (3) 175:5;210:21;217:12 fall (2) 44:21;121:2 familiar (25) 26:16;35:21;36:3;48:11, 12;49:3,5;116:19;117:5;</p>			

61:3;86:8;210:10 found (9) 16:15;118:15;120:17; 121:12;164:15;183:14; 184:1,5;220:5 foundation (3) 22:18;119:6;132:8 four (2) 28:3;84:3 fragmentation (1) 193:2 fragmentations (1) 193:6 fragmented (1) 207:9 framework (2) 31:20;35:2 Free (5) 10:1;129:4;164:17;179:3; 186:5 freeware (9) 144:1,2,3,6;183:10,10,11, 12,14 frequently (3) 195:11;203:6,7 friction (1) 217:4 friend (1) 46:20 front (1) 192:17 FSE (9) 188:5,7;189:15,16; 198:17;209:4;212:2,5; 217:2 FSEs (2) 200:19;218:10 FSE's (1) 219:4 Ft (12) 111:14;112:10;115:21; 122:2;123:18,20;124:6; 127:14,21;128:15;129:5; 189:9 FTB (1) 48:16 FTP (8) 18:13,14;82:17;94:17,18, 19;95:8;96:1 fuel (3) 173:21;174:20;175:2 fulfill (1) 43:21 full (6) 19:13;69:8;197:21;198:5; 216:21;217:16 fully (1) 80:3 function (4) 76:17;78:14;163:7,11 functional (2) 85:15;111:7 functions (4)	34:15;55:12;77:2;97:15 fundamental (1) 62:14 funded (1) 93:16 funding (2) 84:2,4 funny (2) 180:20;192:3 further (11) 12:13,14;20:4;52:1; 73:17;83:8;86:11;99:19; 124:13;178:11;185:19 fusion (2) 68:16;80:18	69:15;73:17;91:11 given (8) 30:4;42:12;45:12;116:8; 119:12;163:17;168:12; 193:1 gives (1) 147:5 giving (5) 47:5;48:9,9;72:3;104:21 glad (1) 148:15 global (1) 24:13 goals (1) 72:10 goes (6) 8:11,12;62:19;98:18; 109:12;171:4 good (11) 18:5;19:10,11;21:14,15; 52:5,6;83:11;148:8;196:6; 202:8 Google (1) 198:3 governed (1) 120:1 Government (31) 2:4;3:3;30:3;31:2,2,3; 33:3,8,10;34:3,9;44:11; 50:5;67:5,9,10,13;75:12; 90:1;120:12;121:8,14,16; 126:4;128:12,16;129:6; 131:17;141:18;147:19; 148:20 government's (3) 121:15;129:13;134:16 grant (1) 46:21 granted (2) 46:9;210:13 great (1) 148:14 greater (1) 56:10 Greg (2) 21:5,12 GREGORY (2) 4:7;21:7 Ground (5) 66:16,19;69:19;80:18; 93:15 group (1) 53:14 grouped (1) 53:9 groups (3) 53:9;54:5;89:20 Guard (1) 28:19 guess (12) 63:10;80:4;125:10;147:1; 190:7;191:3;199:19; 205:13;206:18;207:3;	216:5,19 guest (1) 16:10 GUI (1) 200:4 guidance (5) 51:9;55:12;104:18,21; 117:1 guidelines (2) 23:16;117:10 guy (1) 54:8 guys (4) 53:7;59:13,13;170:13
	G		H
	G6 (4) 55:21;162:3,10,13 gain (6) 15:18;19:16;20:1;40:17; 46:7;174:4 gained (1) 15:15 gals (1) 59:13 game (1) 181:1 games (26) 58:21;103:19;153:11,12, 14,18;156:3,10;163:4,7,7, 11,16;164:12;178:17; 180:12;181:17,18;182:5; 183:13,17,20;185:14;214:8, 15,19 Gammage (1) 197:13 Garrison (1) 1:9 gate (1) 90:20 gates (4) 71:20;75:21;88:9,10 gather (2) 48:17;190:6 Gatorade (1) 202:17 gave (1) 166:18 general (11) 23:1,13;24:20;31:3;40:9; 54:7;170:10,14;171:10; 183:21;196:16 Generally (4) 45:6;53:10;196:13;200:2 generated (1) 17:18 generic (1) 118:10 Georgia (1) 111:14 gets (3)		habit (1) 215:20 hack (1) 191:15 hacker (2) 15:20;53:12 hacking (1) 174:5 half (2) 68:2;222:13 Hall (1) 1:10 Hammer (50) 112:17,18,21;113:4,6,18; 116:3,6;117:13,18;118:1; 122:11;123:11,16;124:2,7; 126:1;130:16;132:6,15; 134:8,17,18;135:7,19; 136:12;137:9,11,20;138:8, 18;139:7,12;142:11; 145:17;176:19;188:17,18, 21;189:5,13,16,18;190:12, 17;191:19;199:3,6,10;201:8 handing (6) 10:10;14:3;19:7;29:5; 128:20;129:17 handler (1) 24:14 handling (1) 25:12 happen (6) 91:19;99:8;161:20;193:9; 210:6;214:3 happened (6) 112:12;122:13,18; 162:15;198:10;210:1 happening (1) 167:20 happens (10) 76:1;77:7;85:11;92:17; 98:2;123:1,6;124:2;141:17; 196:7 hard (20) 13:12;81:21;82:1;164:4; 166:21;193:4,19,19;194:1, 21;195:1,4,4,5;196:8,10;

197:5;207:8,10;222:20 harden (1) 82:4 hardened (1) 82:7 hardware (11) 60:13;71:16;78:3,6; 84:11;99:7;140:16,20; 141:3;196:5,16 hash (17) 8:7,10,14;17:11,15,16,17, 18,20;18:3,7,8,11;19:12,13, 18,21 head (2) 84:7;134:12 Headquarters (7) 1:8,8;70:12,13,13; 122:17;150:21 health (2) 58:5;59:7 heard (2) 162:12;191:2 Hearing (1) 1:15 Hearsay (1) 192:5 heat (2) 202:14;203:3 held (1) 31:5 help (11) 101:21;114:6;121:21; 122:12,17,21;141:20,21; 142:4;144:19;146:6 helped (1) 28:1 Here's (5) 90:18;107:11;132:7; 156:8;210:5 hex (5) 13:14,16,20;15:4;17:1 hey (5) 156:19;207:5;215:6; 220:4;221:10 higher (6) 46:8;56:3,9,15;134:11; 177:3 himself (1) 131:20 hit (1) 90:20 hold (4) 23:21;24:9;25:5;56:19 Honor (42) 6:13,18;11:13;14:15; 18:19;19:1;20:7,9;35:3; 37:20;41:8;48:21;65:1,11; 66:2;83:7;109:20;119:3; 121:1,21;122:5,8;123:1; 124:14;128:10;130:19,21; 131:18;132:13;133:4; 134:14;144:10;145:11; 178:12;180:8;183:6;186:1,	10;192:4;202:3,5;221:16 Honorable (1) 1:17 hooked (2) 169:1;190:9 hoops (1) 94:11 host (1) 16:9 hot (1) 202:20 hours (4) 11:21;12:19;164:16; 187:4 house (2) 193:12;217:9 HPSS (1) 168:6 hub (1) 188:5 human (1) 71:5 hundreds (3) 74:3;162:15;169:6 HUNTER (1) 3:7 HURLEY (6) 3:13;17:6;19:1,9;20:4; 30:8 hurt (1) 182:20	104:18;118:6,9;165:3 identifying (3) 73:8;87:11;89:11 II (1) 121:6 illustrative (1) 129:10 IM (2) 150:7;152:12 image (5) 11:21;12:19;13:2;219:7,8 imaged (1) 196:6 images (3) 14:6;219:5,6 imagine (7) 94:4;149:10;152:16; 156:15;157:8,16;215:11 immediate (2) 159:7;215:13 impact (3) 61:7,8;213:17 implement (1) 59:15 implementation (1) 51:2 implementations (1) 177:14 important (3) 81:5,7;175:2 importantly (1) 179:8 impose (1) 56:10 imposed (1) 44:12 inaudible (26) 2:18;15:8;17:16;21:18; 24:3;26:5;29:18;41:20; 47:4,10;51:3;68:16;69:6; 104:1,3;117:14;121:3,5; 128:4,18;187:10;191:10; 192:6;216:17;217:3;221:7 incident (4) 24:14;25:12,12;46:4 include (1) 224:9 included (7) 19:13,21;117:2;121:20; 132:14;153:8,10 inclusive (1) 42:1 incorporate (1) 28:18 incorporates (2) 23:5;55:12 indeed (1) 55:4 independent (2) 181:18;182:1 INDEX (2) 4:1;5:1 India (1)	176:10 indicate (1) 183:1 indicated (1) 119:11 indicator (1) 25:3 individual (8) 23:13;43:11;56:5,20; 97:11;102:20;120:1;122:16 individuals (1) 152:4 industry (5) 24:19,20;87:16;89:19; 90:3 inference (1) 54:8 information (104) 11:19;12:12;20:2;22:17, 18,19;23:1,1,6,9,11,15;24:4, 6,12,14,18;25:5,11,20;26:2; 27:13;28:10;32:10,12;33:1; 34:16;35:12,13,18,21;36:7, 13,15;39:3;40:4,8;41:16; 43:9,10;44:11,16;48:17; 50:18;51:5,5,12,12;53:19; 69:2,20;80:7;81:19;82:18; 83:1;96:13,15;109:15,18; 111:1,12;112:5;113:13; 114:18;130:11,13;140:4,6, 6;150:2,8,12,17;151:9,12, 14,21;152:6,13;153:1; 159:21;160:11;166:1; 167:1;168:17;169:17,19; 170:21;174:5;176:3,17; 177:11,17;178:2;180:1,6; 182:18;194:1;204:2,5,20; 206:9,10,14 Informations (1) 84:10 informed (1) 72:7 infrastructure (3) 59:12;69:17,21 ingesting (1) 69:19 inherent (1) 82:14 inherited (1) 180:16 initial (5) 27:6;36:7;89:14,16;90:15 initially (2) 80:2;188:16 initiate (1) 166:12 input (1) 89:21 insert (3) 130:12;190:15;194:21 inserted (1) 50:19 inserting (1)
	I		
	IA (23) 28:18;34:16;36:5,9; 37:16;38:1,6;39:4,15;40:6; 41:3;52:20;54:4,8,18;55:9; 114:7,20;150:15,17;183:21; 184:4,5 IAM (9) 150:3;153:1;156:1,15; 162:18;167:8;175:6,8,16 IANCO (2) 178:19;179:7 ID (9) 43:10;44:3;129:18; 132:18;133:5;134:5; 135:15;139:4;170:20 idea (3) 63:6;165:5,7 identical (1) 130:17 identification (15) 14:2,4;29:2,17;65:20; 119:5;126:6;127:6,12; 128:9,12;129:1,7;132:20; 147:10 identified (6) 25:6;39:11;40:13;41:4; 43:18;64:6 identify (8) 42:4;74:6;76:8;87:7;		

50:17 Inside (6) 170:7;174:6,7,10,14; 181:19 insider (2) 45:15;53:12 inspection (1) 23:12 inspections (2) 22:12,12 install (39) 9:6;46:5,13;48:7;51:17; 63:12,13;64:7;101:19; 103:14;105:1;106:3,7,19; 107:3,10,17;137:7;140:19, 21;141:3,4,14,17;142:2,12; 143:7;155:2;160:21;161:5; 198:5,7,15,15;199:10; 200:5;201:5;209:9;212:7 installation (14) 43:5;60:12;82:2;106:10, 14,16;107:8;127:14;128:2; 142:17,18;147:15;154:3; 199:20 installations (3) 126:13,15;134:12 installed (13) 42:16;46:1;106:4;107:1; 137:3;198:4;201:20;212:7, 10,11;219:20;221:5;222:2 installing (2) 35:11,12 installs (1) 68:13 instance (8) 97:16;131:1,9,11;180:5; 209:1;219:6;221:8 instant (1) 41:19 instead (2) 131:10;211:13 instill (1) 28:9 Institute (1) 67:3 instituted (2) 36:16;37:13 instructions (4) 52:13,14;99:12;106:10 integrated (6) 68:12;74:5,6,9;77:10; 86:21 integration (1) 37:18 integrity (2) 22:21;43:3 intelligence (15) 56:1;66:17;67:19;68:13, 15;69:8,12,15;70:11,15; 71:5;75:18;80:18;190:5,7 intend (2) 121:16,19 intended (1)	41:17 intent (7) 42:3;58:17;60:16;136:1, 2;140:5;181:5 intention (1) 54:20 interaction (1) 107:3 interactive (1) 200:4 interest (1) 194:20 interested (1) 17:3 interface (1) 107:16 internet (8) 9:15;10:1;41:19;54:6,6; 62:19;107:9;144:4 interpretation (2) 55:1,3 into (25) 6:17,21;8:2,11,14;16:5; 18:20;59:4;65:12,17;74:15; 75:1;77:4,15;86:19;108:12; 111:19;131:4;158:6,20; 166:3;173:20;182:19; 184:2;191:15 introducing (4) 60:3,4,10;136:15 introduction (1) 212:3 intruded (1) 25:17 intrusion (1) 25:13 investigate (1) 161:7 investigation (1) 116:12 involved (6) 73:7,10;76:15,16;157:3; 187:12 IP (1) 107:13 IPT (11) 75:7,19;76:18,18;87:4, 17;88:5,13;89:1,7,13 IPTs (4) 88:12,17;89:4,8 IPT's (1) 89:12 Iranian (1) 54:1 Iraq (6) 112:17;117:12;119:12; 124:2;188:2,6 Iraqi (1) 184:2 ironed (1) 217:5 ISO (4) 9:16;12:1,20;13:1	issued (2) 105:6;168:6 issues (13) 6:6;40:7;109:7,18,21; 131:15;191:18,21;195:8,10; 196:19;224:9,10 items (1) 30:5 J jabber (4) 211:4,8,9,13 Jacqueline (2) 6:19,21 January (1) 92:7 JASON (4) 5:17;186:7,13,18 Jersey (1) 67:2 job (6) 44:16;79:8,13;80:8;96:9; 189:16 Joint (2) 1:10;71:9 Jon (2) 6:14,16 JOSEPH (1) 3:5 JOSHUA (1) 3:12 JROC (1) 71:9 JSS (1) 188:16 JTFG (1) 26:12 Judge (2) 1:18;37:21 judicial (3) 29:19;30:3;38:1 June (7) 1:16;4:2;5:2;6:19;65:15; 108:10;188:11 junior (2) 57:8,10 justifying (1) 43:20 K Kearns (1) 159:10 Keep (2) 50:14;51:8 kept (1) 182:7 kick (1) 103:8 kind (14) 40:4,13;42:21;56:5; 59:16;62:20;64:10;96:6;	103:19;156:2;164:19; 193:12;200:7;203:1 KITZ (12) 4:13;66:6,8,13;83:11,14; 96:18;99:20;105:15;106:1, 3;107:21 knew (4) 164:1,19;191:16;220:12 knowledge (19) 38:5,10,12;49:1;82:16; 83:5;94:20;99:17;108:2; 131:8;133:14;137:19; 138:17;160:2,16;164:11; 165:10;213:19;223:15 known (3) 17:17;42:13;111:12 L label (1) 152:17 labels (1) 130:9 ladies (1) 59:14 Lafayette (1) 66:21 laid (1) 132:8 LAN (1) 144:20 language (2) 58:15;86:7 languages (1) 86:2 laptop (4) 68:16;69:16;70:6;100:18 laptops (3) 69:7;82:9;189:19 large (6) 68:21;69:4;72:21;73:15; 89:2;207:4 larger (2) 69:2;75:17 LaRue (2) 6:14,17 last (12) 6:4;21:19,20;22:1;35:3; 50:10;108:20;133:18; 142:16;185:19;224:3,12 later (1) 164:16 latest (3) 220:13,15;221:2 Laughter (1) 58:1 law (1) 71:8 laws (1) 58:18 lawyers (2) 65:7;108:3 laxity (1)
---	--	--	---

182:8 lay (2) 69:14;70:3 lays (1) 72:20 lead (9) 22:2,5;68:12,14;76:18, 19;198:17;209:4;212:5 leader (1) 67:16 leadership (1) 57:5 leadership's (1) 57:6 leading (1) 49:15 learn (1) 192:12 learned (2) 22:13;192:9 least (10) 10:4;37:6;121:12;172:14; 180:14;196:1;203:18,21; 207:17;212:16 leave (2) 165:7;216:17 leaving (2) 26:20;180:5 left (1) 196:21 leftover (1) 158:12 legal (1) 33:6 legally (1) 161:4 lengthy (3) 91:13,15;219:2 less (3) 164:9;168:11;182:11 lessons (1) 22:13 letter (6) 101:9,12,20;102:19; 156:20;217:1 letters (4) 15:1,19;210:8,9 letting (1) 183:1 level (14) 8:20;9:1;24:16;37:13; 46:8,14;55:7;56:3,9,16; 70:9;73:1;171:15 levels (1) 45:4 liability (1) 121:9 license (7) 142:1,3;161:3,5,17,20; 162:1 licensed (1) 101:14 Lieutenant (2)	159:10;221:1 lifetime (1) 218:19 light (1) 119:7 liked (2) 220:13;221:1 likely (2) 118:2;157:12 liking (1) 191:9 limit (2) 44:12;167:1 limitation (6) 151:20;152:2,5,12;169:2, 5 limitations (1) 61:17 limited (2) 41:19;44:14 limits (3) 44:10;152:3,4 Lind (1) 1:18 Line (9) 11:10,19;12:4,12,18,20; 14:20;114:3;165:6 link (3) 63:18;64:3;70:4 Linux (12) 9:4,10,15;10:1,3;11:2; 13:4,8,13;15:21;16:11; 190:15 list (3) 30:4;101:3,5 listed (3) 53:10,11;118:20 listen (1) 132:12 listening (1) 2:7 literally (1) 194:14 little (16) 12:13;20:14;45:15;52:20; 68:9;73:6;95:21;103:2; 109:14;135:3;150:19,20; 151:5;153:2;197:7;210:9 live (1) 2:7 load (13) 61:21;62:2,9;63:20; 101:8,8;102:4,21;103:9; 199:1,2;210:17;219:14 loaded (4) 96:1;100:7;102:19; 208:21 loan (1) 68:5 local (15) 11:21;18:17;48:19,19; 56:15;103:12;127:3; 134:12;140:7;144:21;	147:6,15,16;158:17,18 locate (4) 116:13;120:5,6,8 located (3) 15:10;93:14;189:20 location (5) 60:8;137:6;147:14,14; 169:19 locations (3) 169:7;170:9,11 locked (1) 8:16 log (12) 8:2;10:7,18,19;12:2,7; 36:21;63:21,21;139:1; 193:18;194:8 logical (1) 147:3 logistic (1) 224:9 long (21) 23:18;24:9;25:19;27:15; 32:1;33:17;37:10;67:5; 68:8;72:12;78:17;94:9; 111:11,15;133:11;162:7; 166:14;187:19;188:12; 191:9;196:12 longer (3) 126:16;134:18,18 longstanding (1) 25:9 look (11) 59:17;87:19;98:15; 117:19;128:11;129:19; 130:17;147:19;164:8; 173:8;206:20 looked (3) 129:2;146:11;185:17 looking (12) 13:3;32:16;75:12;88:13; 125:12;183:15;184:11,14; 185:4,14;206:18;215:20 looks (2) 88:19;131:3 lose (1) 222:18 lost (1) 151:17 lot (17) 72:5,6;79:8;84:16,18; 90:16;91:16;95:1;99:6; 101:11;193:10;197:7,8; 203:12;204:2,4,14 low (1) 70:10 lower (1) 109:14 Loyalty (1) 188:16	6:7,9,10;17:9;20:12;21:1, 4;29:16;30:1,8;31:8;32:3; 38:4,11,16,19;40:1;50:4,10, 13;52:3;61:13,18;62:2,14, 18;63:2,5,16;64:13;65:9; 66:5;101:6;102:5;103:4,7, 14;104:12,13;105:8;108:4; 109:3;110:2;123:13;127:7; 129:9;134:20;148:19; 180:9;181:13,15;182:9; 183:2,4;186:6;223:10,11, 17,18;224:15 Mac (1) 16:11 Macbook (1) 10:5 machine (33) 16:6,7,8,10,11,17,18,19; 96:20;98:16;106:5;139:1; 158:17,18;189:21;190:4,14; 191:10;193:7;196:6,11; 197:10,21;198:8,11;200:14; 207:15,16;212:8;216:4; 222:17,20,21 machines (22) 63:11,12;97:12,18;98:3, 11;145:3,5;190:2,8,11; 197:11,20;200:18;201:15; 203:8;212:10,12;216:20; 217:17;219:5,15 MacIntosh (3) 10:4;14:11;16:16 Madaras (16) 192:1;195:9;196:18,21; 205:1,3,10,17,20;206:5,19; 207:19;208:1;222:5,7; 223:1 Madrid (1) 110:20 mail (1) 34:11 main (3) 181:6;188:5;189:18 maintain (3) 25:4;81:16;149:19 maintained (2) 25:10;122:11 maintenance (2) 113:10,15 MAIS (2) 69:1;84:9 MAJOR (8) 3:4,13;20:21;84:9; 157:14;159:8,11;202:14 majority (1) 182:1 makes (4) 56:14;72:9;73:20;77:8 making (4) 13:12;147:1,3;215:19 mal (1) 181:5 malicious (6)
		M	
		ma'am (60)	

35:15;60:15;61:10;63:8; 19:147:20 maliciously (1) 64:7 malware (4) 40:12,18;58:20;61:9 man (1) 34:20 manage (4) 57:6;80:19;93:17;149:19 managed (1) 171:16 management (1) 157:4 managements (1) 113:11 manager (26) 7:15;66:18;67:17,20; 68:7;70:18,20,21;71:7,12, 14;72:4;76:4,5,11;77:7; 79:12;81:2,6;93:12;102:15; 111:12;113:13;144:16; 150:2;153:2 manager's (1) 79:8 manages (3) 71:6;93:11,15 managing (3) 79:8,11;81:2 mandate (1) 33:20 mandated (1) 30:19 manner (5) 32:9;41:17;48:6;58:10; 169:21 MANNING (38) 1:6;16:3;31:16;50:2; 112:21;115:10;116:10; 131:15,20;132:3;137:9; 141:11,14;142:12;143:11; 174:3;190:19;191:5,18; 194:10;195:8,12;196:18; 197:17;198:7;201:11,17; 205:3,7,17;206:5;207:20; 212:12,17;222:5,9;223:1,1 Manning's (12) 14:11;16:15;38:5;52:16; 116:13;120:5;121:11; 125:17;190:21;191:12; 196:14;206:19 many (17) 23:5,10;27:9;51:6;56:15; 61:7;63:2,16;73:7;80:12; 115:18;128:6;187:4; 190:11;195:19,21;197:5 March (3) 12:9,18;29:11 MARK (4) 4:13;66:6,8,13 marked (4) 30:2,6;126:5;127:11 market (3)	89:20;90:2,17 Marvin (1) 197:13 Maryland (3) 1:17;66:13,17 master (1) 166:16 master's (2) 67:1,11 match (1) 17:20 material (1) 87:7 mathematical (2) 8:7;17:16 matter (8) 1:15;24:5;74:10;119:7; 128:19;131:12;135:11; 169:17 matters (2) 71:11;119:2 may (43) 2:14;9:20;15:20;19:4; 25:16,17;30:9;44:21;51:14; 62:5;63:6,19,20;64:4;74:18, 20;78:5;87:12,13,14,17; 88:2;92:2;93:19;94:2,8,13, 14;95:6;117:19;123:13; 124:21;130:17;133:2,10; 135:21;158:13,16;172:4; 182:19;193:3,5;219:1 maybe (7) 44:15;121:10;135:2; 172:21;174:17;183:5; 206:12 Meade (1) 1:17 mean (23) 7:19;9:9,12;13:1;24:15; 67:12;69:14;81:21;82:20; 83:19;96:20;134:9;138:11; 140:18;149:9;166:5,6; 168:20;172:5;177:20; 197:19;206:10;211:11 meaning (1) 131:3 means (6) 33:8,9;82:7;84:12; 140:19;171:8 meant (2) 118:11;193:13 measurable (6) 73:21;74:15;75:2,8;86:1, 6 measure (4) 23:8,10;75:2;87:21 measures (1) 59:15 mechanisms (3) 46:3,11;64:15 media (16) 2:7;50:17,18;153:2,5,8; 159:5,13,16;160:17;164:18;	165:4;181:3,15;184:18; 185:1 medical (7) 28:19;33:7;173:4,5; 174:1,19;175:3 meet (15) 71:15;72:1;73:9;75:14, 19;79:2;81:11;82:5;86:5; 87:7;88:4,9;89:12;90:17; 171:8 meeting (1) 81:17 member (7) 26:5;139:19,21;160:19; 169:10,12,12 members (2) 89:19;216:11 memoranda (1) 104:15 memorandums (1) 210:9 memorized (2) 49:12,18 memory (25) 49:14;120:19;121:21; 124:1,9,11;130:15;132:11; 135:7,8,11,18;136:11; 142:11;146:12,17;148:7; 149:6;154:4;190:11; 207:18,19;210:18,19; 211:19 mention (1) 54:1 mentioned (13) 19:19;71:3;73:1;74:5; 76:18;79:4;80:17;82:4; 83:18;85:16;86:2;96:4; 104:15 mentor (2) 197:12,13 merit (1) 56:2 message (1) 103:12 messaging (1) 41:19 met (2) 126:14;224:5 method (3) 44:4;176:17;177:11 methods (2) 40:10;202:17 metrics (3) 23:8,10;78:18 Microsoft (14) 7:15;13:17,18;45:10; 70:5;87:17;88:7;101:14; 107:14;111:21;181:15; 198:3;200:5,8 Middle (3) 112:19;127:19;222:12 might (17) 40:11;43:19;48:5;63:19;	64:8;80:13;85:5;131:3,10; 145:15;151:15;168:17; 172:20;174:17,19,21; 215:12 military (9) 21:16;22:1,6;69:8,15; 186:21;187:5;216:10;217:9 Miller (5) 156:5,8,16;157:19; 209:15 MILLIMAN (8) 5:17;186:7,13,18;202:7; 208:9;220:4;221:13 mind (1) 60:16 mine (7) 64:21;104:11;116:17; 125:19;126:14;171:11,12 minute (1) 178:12 minutes (5) 10:16;133:12;148:4,7,21 mIRC (37) 101:3,11,19;102:21; 105:12,15;106:7,8,12,21, 21;107:2;153:20;154:4; 156:10,17,20;157:20; 209:19;210:4,11,16,17; 211:3,6,12,20;212:3,13,17; 218:3,4,13;219:8,15,18; 221:19 mirroring (1) 48:18 mischaracterize (1) 104:17 missing (2) 2:17;161:8 Mission (8) 22:15;44:17,19;64:9; 94:11;157:2;160:20;213:18 misspelled (1) 2:16 misunderstood (1) 106:20 mitigate (2) 59:15;79:6 mitigating (1) 59:10 MNFI (1) 171:16 modification (1) 41:15 modifications (8) 42:21;43:1;136:6;137:4; 140:15;141:5;200:6,12 modified (1) 181:7 modify (4) 46:5;96:20;127:3;166:14 moment (8) 57:13;83:7;122:4;133:2; 144:10;145:13;154:8; 179:11
--	--	--	---

moments (1) 18:5	moving (5) 61:2;64:17;98:21;140:3; 158:19	144:17	220:9
Monday (2) 224:12,20	MSCI (1) 107:4	neck (1) 109:14	newest (1) 185:7
money (1) 84:18	MSI (5) 106:9;107:5,6,7,15	need (44) 6:6;9:14;19:20;33:14; 43:18;81:9,10,19;85:6,19; 86:10,14;87:13;88:4;96:9, 12;107:13;114:4,16; 115:15;123:4;143:4;148:6; 154:16;155:2,16,19;156:19; 160:21;165:16;167:7; 172:6;173:3,5;174:9,13; 176:21;179:11;190:6; 196:10;201:3;207:5; 212:12;224:17	newly (1) 22:8
monitor (1) 57:7	much (9) 47:15;147:10;163:8; 164:7;173:21;175:2,3; 195:11;204:20		next (10) 6:8;16:20;63:21;74:1; 106:11;107:11,12,15;110:5; 130:20
monitored (1) 178:15	multinational (1) 171:15	needed (14) 19:18;39:6;47:18;84:12; 114:2,18;159:16;160:4; 174:15;196:13;198:13,13; 219:15;222:19	night (5) 115:13;124:20;222:6,9, 13
monitoring (1) 188:6	multiple (6) 11:5,8;73:9;80:18;82:19; 88:12	negligent (1) 182:18	nine (2) 27:16;111:16
month (2) 127:15;197:2	multitude (1) 40:6	nervous (1) 194:5	NIPRNET (1) 136:4
months (7) 24:10;27:16;92:8,13; 111:16;164:16;188:13	music (25) 57:16;58:14,15,17;61:11; 103:19;104:4;153:8;156:9; 158:1;163:16;164:5,12; 178:16;180:20;181:2,3,14, 16;182:5;183:20;185:14; 214:9,12,19	nest (1) 81:13	noncombat (1) 21:18
morale (1) 58:5	Myer (1) 1:11	nested (2) 126:14;134:8	noncommissioned (1) 21:17
more (15) 19:18;46:18;89:12;105:5; 145:11;147:11;164:9; 168:11;179:8;180:8; 182:11;195:11;202:3,18; 220:18	Myer-Henderson (1) 1:10	net (4) 138:2,4,5,9	none (6) 30:5;65:2;163:21;165:14; 166:1;197:16
morning (2) 205:11;224:12	myself (3) 74:12;157:7;170:13	nets (1) 171:9	non-INAUDIBLE (1) 22:21
MORROW (18) 3:5;7:2;10:8,12;11:12,15; 14:1,5,14,17;18:19;19:7; 20:7,9;21:2;157:14;159:8, 11	N	network (60) 22:14;24:6;25:16,18; 28:10;31:2;34:5;42:16; 43:20;44:3;46:21;48:8; 58:18;60:9;61:1,2,6;62:10; 63:9;80:20;81:18,20;82:6; 100:10;113:11,15;114:4; 115:7;118:14,14,16;124:3; 130:12;136:16;137:6; 138:7;139:11,15;140:13; 144:20;160:14;165:16; 171:16;178:9,16,20;179:9, 17,19;180:2;181:9;183:10, 12,16,20,21;185:13;190:8; 195:1;217:11	nonofficial (1) 34:9
MOS (1) 187:7	name (10) 11:21;95:16;118:13,14; 130:12,12;186:18;192:1; 197:12;209:16	networking (1) 111:20	normal (3) 8:17;45:6,20
most (15) 15:21;72:9;77:1;80:4; 92:11;106:11;118:2;119:6; 131:9;147:15;157:12; 163:10;178:18;203:20; 223:7	names (4) 2:16;7:17;17:5,11	networks (8) 25:13;40:17;59:7;81:10, 11,14,15;113:17	normally (7) 44:6;45:4;63:12;121:14; 200:3,5;202:2
mount (1) 13:12	National (1) 28:19	new (26) 26:7;67:2;82:1;87:14; 90:7;92:6,10,14,16;98:19; 99:6,8;109:1,21;117:9; 176:19;194:2,21;195:4,7; 207:14;216:18;219:5,7,7,8	north (1) 169:13
Mountain (13) 52:16;112:9;120:13; 136:4;139:20;169:11; 189:4,5,14;197:14;209:12; 210:14;212:9	NATO (1) 110:19	newer (1)	notes (2) 2:15;219:9
Mounting (1) 13:12	nature (1) 42:1		notice (3) 29:19;30:3;38:1
move (12) 18:19;71:20;95:11,17,18; 96:1;100:1,5,7;110:3; 194:7;207:5	Naval (1) 84:8		noticed (1) 214:11
moved (2) 60:7;109:3	navigate (2) 9:7;13:13		notified (2) 159:7,10
moves (1) 65:19	navigated (1) 16:21		notify (1) 183:19
movie (3) 62:20;63:6;180:20	NCIC (1) 146:7		November (3) 23:20;112:19;187:18
movies (13) 153:10;156:3,10;158:1; 164:5,12;178:16;180:12; 181:3,11,16;183:20;214:9	NCO (2) 164:19;170:13		number (12) 22:15;38:2;39:12;43:1; 46:12;53:13;60:6;84:5; 86:17;88:14;97:3;135:14
	NCOs (1) 164:1		numbers (4) 14:21;15:13,19;53:14
	NDAP (1) 84:8		numerous (1) 47:2
	necessarily (4) 44:1;60:11;99:3;106:5		NWR (2) 34:11;156:8
	necessity (1)		O
			oath (1) 7:11
			object (7) 31:15;34:19;37:20;48:21;

<p>50:1;120:10;134:14 objecting (1) 49:2 Objection (12) 17:6;19:1;30:7;32:5;66:1, 2;119:7;120:21;129:8; 132:9;133:7;192:4 objectives (1) 77:5 objects (1) 119:4 obligations (1) 36:14 observe (3) 11:1;12:7;109:19 observed (2) 12:8,8 obtain (3) 144:4;149:9;162:4 obtaining (2) 142:7;161:7 Obviously (14) 28:14;37:8;42:19;44:12; 46:13;47:4;53:19;57:6; 58:11;96:10;121:4;151:15; 158:15;214:3 occasionally (3) 178:19;203:15,16 occur (1) 48:5 occurred (1) 25:18 occurrence (2) 44:17;216:14 occurring (1) 168:4 o'clock (1) 20:17 October (1) 112:11 odd (2) 196:2,3 off (10) 9:5,14;63:21;83:1;84:6; 124:3;164:11,12;202:18; 215:6 offense (3) 121:6,7;128:18 offer (3) 130:19;131:4;133:4 offering (2) 38:5;124:9 offers (5) 6:10;29:17;40:2;65:12; 108:5 offhand (1) 105:3 office (11) 24:4;45:10;66:17;70:5; 77:2;87:18;101:14;107:14; 198:4;200:6,8 Officer (16) 6:14,16;21:17;109:11,16;</p>	<p>110:19;113:7,12,13;149:16; 150:1;157:7,10;166:10; 175:11;221:4 officers (1) 163:21 officer's (1) 173:4 official (3) 2:4;101:9;198:19 officials (2) 28:16;51:15 often (3) 178:20;195:8,9 old (7) 92:3,8;99:2,7,9;194:21; 195:3 older (1) 92:14 Once (23) 16:19;20:10;62:12;90:20, 20;91:9;92:9,12,14;93:8; 103:7,14;104:8;122:19; 123:6,18;145:16;152:19; 163:8;194:18;195:2;196:5; 211:21 one (88) 11:6;14:10;23:11,12; 24:1;29:14;31:14,17;40:7; 46:12;49:12;55:13;57:13; 58:19;59:18;60:6;68:11; 83:7;84:5,13;87:10,20;89:4, 7,12;92:15;93:1,2;97:11,16; 105:5;118:12;121:12; 125:10;126:2,17,19;127:21; 128:3,17;131:6;132:21; 134:10;135:14;139:1; 142:16;143:13;144:10,13; 146:13;147:19;149:4; 151:19;161:6,7;162:2; 163:20;166:15;170:12; 176:7;177:1;178:12;182:2; 183:13;184:1;185:11; 191:7,14;193:20;204:1,4, 13,14,16;205:5,11;207:14; 208:6,13;211:19;216:17; 220:1,2;221:21;222:5,6,20, 20 ones (1) 217:16 online (3) 36:17;150:15;220:5 only (34) 15:9,18;18:11;45:3; 56:15;94:19;97:16;100:2,3, 13;102:5;116:15;119:20; 129:10;135:1;138:21; 152:2,7;161:17;162:19; 166:15,17;174:17;191:2; 194:6;204:5,19;208:6,13; 213:15;215:9;216:1;217:2, 15 onto (13) 63:20;105:16;141:18;</p>	<p>142:12;143:9,11;151:21; 152:13;158:8;208:10,16,21; 218:3 op (1) 22:3 open (5) 54:21;55:2;64:11;87:18, 18 Opening (1) 12:3 operate (7) 100:5,15,17;155:3;181:4, 10;199:18 operating (21) 7:16;9:5,11;10:1,4;11:2; 13:4,10,13;16:10;31:6; 47:7;92:2;137:4;140:20; 141:5;190:15;193:21; 196:9;207:3;216:3 operation (4) 46:2;64:18;100:6;110:19 operational (9) 23:14;64:14;77:15,16,17, 18;78:13;90:21;139:14 operations (4) 22:2,3;100:14;111:5 opinion (4) 57:19;182:8,9;214:2 opportunity (2) 59:9;207:13 opt (1) 207:15 opted (1) 165:20 Oracle (3) 102:9,10,12 orchestrates (1) 89:2 orchestrating (1) 89:8 order (21) 2:11;6:2,5;19:16;20:20; 39:5;46:6;72:1;80:10;81:9; 82:5;108:18;114:1,9,13,17; 120:14;133:17;197:2; 207:11;208:18 orders (1) 150:5 ordinary (1) 198:2 organization (7) 22:8;23:14;26:8;33:12; 34:3;68:3;138:6 organize (1) 74:4 organizing (1) 74:1 original (2) 18:16;63:10 originally (4) 26:3;60:6;122:13,18 OS (1) 82:7</p>	<p>OSD (1) 71:20 others (4) 115:9;191:3;196:14,15 otherwise (2) 165:19;207:6 ought (1) 121:9 out (47) 11:5;15:20;18:17;21:19; 26:7;37:3;67:10;72:20; 74:7;78:5;82:11;87:13; 90:5,9;92:6;95:1,14;98:6, 18;101:10,18;102:9; 103:11;104:15;112:7; 114:2,13,14;119:6;175:2, 14;185:5;189:16;193:4,19; 194:21;196:8;198:19; 201:20;203:8,11;207:9; 209:7;217:5,7;220:5; 222:19 outline (3) 31:4,4;72:21 outlined (2) 101:7,12 outlines (6) 2:14;30:21;32:12,21; 33:4;45:19 outright (1) 59:16 outside (7) 35:13;40:13,15;170:18, 18;174:6;183:16 over (11) 23:19;24:10;28:2;68:9; 69:6,7,18;98:21;148:21; 180:17;194:3 overcame (1) 202:16 OVERGAARD (1) 3:6 Overlap (1) 216:17 override (1) 32:4 Overruled (2) 17:10;38:21 oversees (1) 68:19 oversight (5) 76:17;77:3;84:16;91:16; 175:17 own (8) 39:19;74:7;118:11;126:7, 10,11;199:18;213:17 ownership (1) 99:10 owns (1) 33:12</p>
P			
package (8)			

175:21;176:8,13,15; 177:9;210:5;211:4,6 packages (1) 176:7 Packet (1) 176:4 Page (8) 4:4;5:4;11:16;12:10; 29:14;41:11;119:2;130:8 pages (5) 32:15;39:15;95:15,19; 128:6 PaPa (1) 176:11 paperwork (3) 177:13,18;180:3 paragraph (16) 34:13;41:14;45:18,18,19; 49:10,21;50:9,11,16; 132:10,10,21;135:14,20; 136:9 paragraphs (2) 54:17;133:9 parameters (7) 44:18,20;45:1;46:1;64:1; 76:13;137:17 part (33) 7:15,17,19;8:11,12;15:4; 17:11;18:11,16;19:20; 32:11;36:11;44:16;46:1,2, 20;55:10;64:13;83:16; 84:21;91:11;95:2,9;101:13; 155:11;156:21;175:20; 177:21;178:18;203:20; 208:21;210:5;211:4 particular (7) 40:10;41:6;54:6;104:18; 218:9,20;220:14 parties (7) 6:3;20:21;21:1;133:18; 224:3,5,13 parts (2) 8:11;76:16 pass (1) 37:8 passes (1) 8:6 password (15) 7:18,20;8:3,6,14,14; 17:12;18:3,6;40:8;103:9; 168:18;216:11;217:6;221:6 passwords (7) 8:9;17:15,20,21;19:17; 20:1;43:11 past (6) 53:9;97:6;214:11;216:10; 218:2;220:12 patch (1) 102:12 patches (1) 216:3 patching (1) 42:13	pay (2) 144:5;217:20 peninsula (1) 54:2 Pennsylvania (1) 110:15 Pentagon (1) 21:19 people (9) 8:9;14:3;61:6;100:2,3; 146:3;181:5;185:6;191:16 people's (2) 120:8;173:4 PER (1) 88:9 percent (1) 207:21 perform (2) 23:15;25:12 performance (5) 34:7;76:13;79:14;88:1; 193:3 performed (1) 179:8 performing (1) 88:2 period (3) 78:17;164:17;174:1 periods (1) 164:15 permanent (5) 20:8;65:3;107:19;185:21; 223:12 Permission (10) 11:12;14:14;31:7;41:7; 45:4,6;51:11,19;134:1; 199:7 permissions (2) 45:8;62:4 permitted (8) 2:5,8;32:13;52:17;57:16; 115:6;151:11;171:19 person (11) 18:11;19:16;50:21;51:4; 71:1;98:15;102:6;140:14; 150:7;168:21;213:12 personal (8) 14:11;16:15;35:16;49:1; 50:5;51:1;94:19;131:8 personally (4) 162:14;164:1;178:19; 179:1 personnel (4) 22:6;35:16,16;50:21 person's (1) 185:15 perspective (2) 72:19;98:8 PFC (49) 1:6;14:10;16:3,15;31:16; 38:5;50:2;52:16;112:21; 115:10;116:10,13;120:5; 121:11;125:17;131:15,19;	132:2;137:9;141:11,14; 142:12;143:11;174:3; 190:19,21;191:5,12,18; 194:10;195:8,12;196:18; 197:17;198:7;201:11,17; 205:2,7,16;206:5,19; 207:20;212:12,16;222:5,9; 223:1,1 phase (9) 86:20;88:19,21;90:19,21; 91:2,5,7;111:21 phases (1) 111:20 philosophy (1) 216:19 phishing (4) 40:9,9,16,18 phonetic (1) 197:13 phrase (1) 147:21 physical (3) 40:19;99:6;152:2 picture (1) 86:10 piece (15) 42:17,17;44:7;46:13; 55:11;70:4;73:8;78:4; 109:1;110:1;137:1;138:6; 141:19,21;161:8 pieces (3) 8:15;75:5;80:19 piling (1) 204:10 Pittsburgh (1) 110:15 place (19) 2:6;11:6;58:3;64:15; 112:20;134:13,21;139:14; 140:6;152:3;170:5;172:13; 176:18;177:15,15,19,19; 189:3;193:20 placed (3) 139:17;151:21;214:12 places (2) 11:5,8 placing (4) 109:8;159:15;160:17; 215:21 plain (3) 8:3,6,9 planned (1) 20:15 planning (2) 111:4;166:15 plans (1) 110:19 play (2) 79:16;181:16 player (4) 104:4;181:16;184:18; 185:1 please (18)	11:19;19:4;20:19,21; 30:10;57:13;65:6;108:1; 111:17;129:19;130:14; 133:13;135:13;136:8; 138:13;186:3;208:9;223:15 plus (2) 22:15;112:6 pm (3) 1:17;99:10;224:21 point (18) 11:5;76:6;82:4;90:3; 124:17;125:4,9,21;126:8; 157:17,19;169:14;177:1; 191:4,7;192:19;212:7; 215:17 points (2) 76:14,20 policies (10) 28:17;30:16;31:1;33:6; 36:9,11;127:3;134:13; 147:7,16 policy (16) 24:8;28:19;30:18,19; 32:7;36:5;51:7;59:8;63:5; 114:15;115:2,5;130:5,9; 135:10;143:20 pool (1) 96:10 poor (1) 193:3 pop-ups (2) 64:4,5 port (1) 195:4 portal (2) 169:14;170:8 portfolio (14) 68:19,20,21;69:5,11;71:2, 6:78:4;80:4,5,15,16,19,20 portion (1) 38:18 position (28) 23:18,19,21;24:9;25:5,7; 55:19;68:10;70:17;72:13; 99:16;110:18;111:3;113:6, 9;129:13;156:1;167:8; 175:11,13;189:13;202:1; 213:10,11,19;215:2,3,5 positive (2) 81:16,17 possess (1) 24:11 possible (10) 92:1,5;93:19;94:4; 105:15;168:8,11;195:3; 209:21;219:18 possibly (1) 222:18 Posted (1) 150:18 potential (1) 63:7 potentially (2)
--	--	--	--

<p>53:18;58:19 practice (5) 147:4;159:15;160:4,8,11 practices (6) 23:17;28:2,5,10;55:9; 150:8 precipitated (1) 206:4 predominantly (2) 22:11;27:2 preeminent (1) 24:16 prejudicial (1) 131:14 preliminary (2) 76:4;88:9 premise (2) 121:8;128:16 prepare (1) 25:15 preparing (1) 12:2 prescribed (1) 32:9 presence (4) 15:12;159:5,12;182:13 present (10) 6:3,4;21:2,3;108:19,20; 133:18,19;224:3,4 press (1) 9:20 Pretty (2) 47:15;164:7 prevalent (1) 216:6 prevent (8) 42:4;79:5;168:3,9; 179:21;180:7;213:12,20 prevented (3) 140:3,9;167:19 preventing (1) 172:17 previous (4) 53:5;158:12;180:17; 197:3 previously (2) 7:6;74:17 primary (2) 26:21;149:18 principal (1) 28:4 principals (1) 28:18 principle (1) 62:14 principles (4) 22:19;34:17;55:9;74:2 print (1) 37:3 printed (1) 30:5 prior (6) 23:21;24:2;37:18;68:10;</p>	<p>125:2;180:15 priority (1) 92:11 privacy (1) 33:5 privilege (1) 61:16 privileged (1) 46:8 privileges (13) 8:21;9:2;46:7,16;47:5; 63:15;137:3;140:15; 141:12;198:5;213:16; 216:21;217:3 Pro (1) 10:5 probably (8) 18:16;54:7;106:9;169:6; 197:6,8;208:1;218:5 problem (7) 59:11;191:8;192:17; 203:4;206:3;207:2,12 problems (13) 144:18;191:8;192:8,10, 12,15;202:10,14;205:14,20; 206:21;222:8,15 procedure (1) 207:3 procedures (4) 24:8;26:10;28:8;31:1 Proceed (4) 108:7,21;134:3;186:11 proceedings (4) 2:6,10;6:1;94:20 process (76) 16:12;43:13,17;46:17; 47:20;48:1;57:4;58:3,7,9, 14;64:14,14,15;71:19;72:9, 15,17,18,20;73:2,18;74:7; 75:17;76:14,16,20,21;78:7, 13,19,20,20;79:5,7;83:4,15; 84:20;87:6,11;89:6;91:13, 15;93:2,9,18;94:6,9,14; 102:8;106:17;112:13,14; 142:17,18;161:1,7,10,19; 162:2,4,7,7,10,13;167:10; 175:20;176:4;178:1;194:4, 6,14;199:21;200:2,4;208:17 processed (1) 42:7 processes (3) 26:9;28:8;93:21 processing (2) 69:12;75:5 processor (12) 74:18,19,20;75:3;85:6,9, 16,18,21;86:10;87:9;88:2 procure (1) 101:16 procurement (2) 70:8;71:18 procures (1) 72:21</p>	<p>procuring (1) 71:8 produce (5) 2:11;120:12;121:10,11; 125:15 produced (1) 131:21 product (12) 68:12,14;70:5;74:5,6,9, 13;76:5,19;86:21;96:16; 101:14 production (1) 73:13 Professional (5) 24:13,17;25:1,2;112:5 professionals (3) 24:18;69:8;70:15 profile (19) 78:14;79:1,4;81:3,3,16; 82:13;193:8,15,17;194:6,7, 8;204:5,17,18,19;207:7,14 profiles (3) 193:6;204:1,14 program (88) 13:18;14:12;17:19;24:4; 52:12,14;66:17,18;67:11, 14,18;68:6,18;69:4;70:6,7, 18,20,21;71:3,4,4,11,14; 72:4,10;73:1,15;75:17;76:4, 11;77:4,5,7;79:8,12;81:2,6; 83:15;84:3,4,8,21;88:8; 89:2;91:10,16;93:11;94:17; 95:8,11,13,16;97:2;98:4,5, 18;102:4,15;103:1,5,10; 137:17;142:9,12;143:8; 155:11;156:21;160:21; 162:19,20;181:4,10;198:10, 14;201:18;208:16,21; 209:2;211:4;212:6;217:14; 218:18,21;219:7,10;221:5; 222:2 programmer (1) 98:7 programming (1) 95:1 programs (13) 69:3;84:13;101:4,6; 154:8;162:15;178:21; 181:1,2,21;198:8;218:6; 219:13 prohibit (4) 34:13;41:14;59:17;88:3 prohibited (12) 35:7;42:21;43:2,4,8,11; 64:11;136:16,17;144:7; 170:16;183:11 prohibition (4) 42:2,3,4;45:20 prohibits (5) 34:14,15;41:15;143:14, 18 project (4) 67:16,16,17,20</p>	<p>proper (1) 42:5 properly (3) 50:20;168:13;175:17 proposals (1) 75:11 propose (4) 75:16,19;76:9;88:5 proposed (4) 76:2,3;88:11;90:10 proposing (1) 71:18 pros (1) 56:6 Prosecution (47) 6:11,12,13,15,20;10:8,10; 11:16;12:10;14:1,3;18:20, 20;19:2;29:1,17;30:11; 38:20;40:21;41:11;51:20; 65:13,16,20,21;66:3;108:8, 11,14;110:6;119:1,4;129:1, 7,17;130:20,20;132:18,19; 133:5,5;134:4;135:14; 139:4;148:18,19;149:12 prosecutor (1) 154:19 protect (1) 51:12 protected (3) 109:15,18;168:18 protecting (1) 50:17 protocol (1) 94:19 provide (3) 78:6;178:9;216:2 provided (4) 31:3;45:14;70:1;80:10 provides (1) 55:14 providing (5) 22:14;69:12,20;82:14; 98:19 Proving (2) 66:16;93:15 publication (2) 27:4;48:3 publish (6) 11:12;14:14;31:7;41:7; 49:16;134:1 published (3) 27:6;33:21;39:17 publishes (1) 29:14 publishing (2) 11:16;12:10 pull (4) 95:18;169:19;194:1,2 pulls (2) 82:18;83:1 punished (1) 160:17 punitive (1)</p>
---	---	---	--

<p>54:17 purchase (3) 70:7;161:18;162:2 purchased (2) 71:17;168:3 purpose (9) 41:17;42:2;49:21;54:17; 78:11,12;178:5,7;190:4 purposes (3) 2:9,16;129:10 pursue (1) 165:8 pushed (1) 18:17 put (37) 71:20;93:1,7;94:12; 103:15;104:7;109:6; 143:11;152:16;154:12; 155:5;156:19;158:14,15; 166:15,21;167:10;193:20; 199:7;200:13,17;203:14; 208:16;211:14;212:13,17; 213:4,13;214:4,7,8;215:9; 216:7;218:3;220:5,10; 221:9 putting (4) 143:8;160:11;213:20; 220:18 puzzle (1) 161:8</p>	<p>RDT (1) 84:3 reach (1) 90:5 reaches (1) 103:11 react (1) 25:16 read (17) 6:17,21;45:7;65:12,17; 108:5,12;131:2;135:13; 136:8;138:13;145:16; 148:3,7;149:1,3;221:21 readily (2) 87:15;142:1 reading (6) 11:7;129:21;135:16; 136:10;138:15;145:21 ready (2) 110:5;186:9 real (2) 111:5;173:5 reality (3) 59:5,6;96:5 really (9) 55:5;70:3;81:7;92:7;94:8; 10;104:5;123:4;191:16 reappear (1) 164:16 reappearing (1) 182:7 reason (2) 165:21;174:20 reasons (4) 25:1;159:18;165:5; 182:13 recall (35) 123:20;125:1;126:3; 136:14;148:1,3;153:19,20; 157:19;185:4,4;195:21; 199:9,12;201:10;205:9,10; 209:17,18,21;210:2,7; 211:1;212:3;214:17;218:5, 12;219:17;220:17;221:3,3, 4,7;223:4,4 recalls (1) 7:2 receive (5) 40:11;45:5;111:9;112:2; 114:17 received (1) 112:4 recent (2) 97:1;220:18 recess (13) 20:14,18;108:17;109:4; 133:10,15,16;186:9;223:19, 20;224:1,11,18 recessed (6) 6:4;20:16;108:20;133:19; 224:3,19 recognize (9) 10:13;14:6;29:7,12;</p>	<p>31:11;39:2,10;41:12;127:6 recognized (1) 24:19 recommendation (1) 104:17 recommendations (2) 44:8;88:18 record (14) 6:3,17;7:1;65:12,18; 108:6,13,19;109:10;118:21; 131:19;133:18;139:3;224:2 recording (1) 2:9 records (3) 122:13,18;173:5 recovered (1) 14:10 recreate (2) 192:17;207:14 RECROSS (6) 4:11,18;5:14;19:9; 104:14;184:10 recruit (1) 9:4 redeploy (1) 160:14 redeployed (7) 117:12;123:7;124:7; 125:7;132:1;189:2,8 redeployment (6) 117:8;125:2;126:9; 134:10,15;135:1 redeploys (1) 98:2 REDIRECT (16) 4:5,10,16,19;5:11,13,15; 20:6;59:20;60:1;99:21; 106:2;178:14;183:8; 185:12;221:15 redlines (1) 55:8 redundancy (2) 88:20;89:11 reference (1) 132:17 referenced (1) 123:4 referring (1) 148:17 refine (1) 74:15 reflect (7) 6:3;108:19;109:10; 118:21;133:18;139:3;224:2 refresh (3) 49:13;148:6,13 refreshing (1) 149:6 regard (2) 79:1;106:13 regards (3) 162:18;174:3;203:17 regenerate (1)</p>	<p>17:17 registry (3) 13:19;103:8;200:7 regular (2) 48:4;153:5 regulation (11) 27:18;33:18;35:9,9; 54:18;55:5;57:18,20;59:4; 143:14;178:4 regulations (6) 29:14;32:16;55:2;115:8; 118:20;127:4 regulatorily (1) 71:21 regulatory (2) 28:8;182:14 reimage (11) 193:7;194:11;195:17,19; 196:11;205:14,16;207:15, 20;212:8;216:4 reimaged (5) 194:19;196:13;207:16, 17;222:21 reimaging (6) 194:4,6,14;197:3;206:1; 222:9 related (4) 27:20;35:17;64:9;112:1 relationship (2) 169:15;170:6 relatively (9) 70:2;82:1;84:6;99:18; 107:1;176:19;197:2,8; 200:1 release (2) 102:10,13 released (1) 101:7 releasing (1) 75:11 relevance (5) 31:16;37:21;50:1;131:5; 134:15 relevant (4) 38:14;93:17;119:8; 131:12 relief (1) 112:20 relies (1) 51:5 reloading (1) 98:20 rely (1) 57:10 remain (2) 81:20;123:3 remains (2) 93:17;98:9 remember (14) 53:5,8,13;84:7;117:21; 180:14;191:7;194:9,11; 196:21;205:10;209:12,13; 220:21</p>
<p>Q</p>			
<p>qualify (2) 102:7;104:19 quantity (1) 147:14 quickly (2) 47:4;195:3 quite (7) 18:12;89:2;90:17;97:21; 126:16;128:14;209:21</p>			
<p>R</p>			
<p>rainbow (5) 17:13,14,16;18:1,4 Ramadi (1) 188:17 ran (1) 213:5 range (1) 166:14 rank (1) 221:3 rapid (4) 27:8,10;29:10;33:19 rapidly (1) 51:7 RAR (1) 33:21 RCM802 (1) 224:6</p>			

remembers (1) 132:12	10,11,19;74:2,8,15,15,18, 19,21;75:2,20;81:14,15; 85:16;86:6,10;88:14;89:12; 95:6;114:21;137:7	retired (7) 21:17,18,18;26:4;187:1,7, 11	roof (3) 193:12,12;204:10
reminders (2) 150:19,21		retrieve (5) 137:16,17;140:6;148:16; 206:8	room (4) 2:7;59:14;109:1;202:21
remnants (1) 158:16	requirements (23) 28:9;71:15;74:4;75:8,13, 14,16;78:13;79:2;81:11,18; 82:5;85:1,4,5;86:17;87:8, 10;126:14;171:9;178:6,7,8	Retrieving (10) 10:8;14:1;29:1;30:12; 38:20;40:21;50:17;118:21; 128:8;134:4	rotation (1) 68:1
remotely (1) 39:6		Returning (4) 41:1;51:20;139:4;149:12	roughly (2) 124:21;190:13
removable (1) 50:18	requires (6) 36:10,11;38:12;44:16; 107:2;154:3	reusability (1) 23:2	rule (1) 50:7
remove (7) 140:2;158:2;172:8,18; 182:5;215:9;217:6	rescind (1) 56:4	review (13) 10:16,19;12:6;76:4,9,10; 88:9,10;89:14,16;90:16; 93:10,18	rules (7) 20:11;28:17;34:5,6;50:6; 118:20;136:5
removed (1) 50:19	rescue (3) 12:1,19;16:15	reviewed (1) 11:1	run (25) 9:5;52:12,18;100:16; 103:18;104:8;137:2,5; 142:20;143:7;154:8,14; 155:3,6,8,15,18;163:9; 167:15,19;181:21;182:3; 196:8;202:20;218:10
removing (2) 140:9;221:6	research (2) 84:3;142:6	revising (1) 146:8	running (4) 8:15;193:4;195:2;207:9
repair (1) 195:12	Reserve (1) 28:19	revision (4) 27:8,10;29:10;33:19	runs (2) 9:6;199:17
rephrase (1) 98:1	reset (1) 98:6	right (46) 18:12;32:4;35:4;38:17; 47:16;51:6;85:9;86:18; 87:21;89:3;90:8,8;92:13; 93:3;96:6;100:13;119:9; 122:3;125:5;129:13; 145:19;146:14,18;147:18; 149:20;151:6,18;152:1; 155:13;162:20;168:15; 170:4;172:9;176:4,5; 202:12;203:19;204:9; 206:15;208:3;211:6;214:5; 216:1;219:3;220:14;221:12	S
replace (1) 118:11	resilient (1) 81:1	rights (25) 97:4;102:6;103:3;104:9; 105:17;140:12,18;142:20; 154:16,20,21;155:3,16,19; 167:8;170:12;197:9,10,12, 15,17;198:5;208:14; 216:21;217:16	S2 (2) 52:15;114:4
replaced (1) 130:11	resource (2) 168:5,8		S3 (2) 166:13,20
replicated (1) 82:9	respect (2) 25:1;180:12		S4 (2) 162:2;173:21
report (2) 22:8;51:13	respond (1) 25:15		S4C (1) 174:20
reported (2) 63:7;184:5	response (6) 25:12;26:6,8,20;192:7,14		S6 (4) 113:5;143:5;156:2; 167:18
reporter (8) 2:4,5,15,19;41:1;51:21; 134:5;149:13	responsibilities (9) 27:1;34:5,6;45:12;51:4; 111:2;113:8,10;188:3		safe (2) 64:16;95:2
reporting (5) 2:14;22:3,11;23:12;26:11	responsibility (16) 25:2;34:8;42:12,20; 44:13,15;50:6,16;51:1,10; 55:13;57:6;136:5;150:20; 157:1;210:4		SAM (19) 7:13,13;8:11,16,19;9:2,7; 13:9,13,19;14:12;15:4,8,10, 15;16:21;17:3;18:8;19:17
representation (1) 74:11	responsible (9) 27:3;28:15;56:20;59:7; 113:14;175:16;188:5; 190:1;201:15		same (16) 16:14;20:11;36:4;39:15; 58:21;80:13;95:13;97:15; 103:5;117:20;133:1,7; 136:1;163:11;193:21;212:4
request (13) 57:7;75:11;92:16;114:14; 128:21;141:19;157:6; 166:11;198:18,20;199:7; 209:3;210:20	rest (1) 222:13	riptow (2) 216:13,15	sample (29) 117:3,5,8,16;118:6,10,19; 119:15,20;120:11,18; 121:21;124:10;126:12,17; 127:2;130:5,9,15;132:5,21; 134:8,11;135:5,9,20; 136:12;138:19;148:11
requested (4) 57:4;58:8;166:10;207:21	Restored (1) 16:16	rise (1) 121:2	SANS (3) 24:13;25:8,9
requesting (2) 102:14;208:20	restrict (1) 213:15	risk (19) 43:6,7;56:7,8,10;59:10, 15;78:14,21;79:4,7,8,9,11; 81:3;101:15;102:18; 105:14;210:10	satellite (1) 70:4
requests (1) 223:19	restricted (3) 166:20;170:12;172:3	Roger (2) 84:17;85:3	satisfy (1) 59:17
require (7) 80:8;103:8;137:4;170:1; 181:3;199:18;224:8	restriction (6) 136:15;166:9,11,12,15; 172:17	role (3) 68:18;77:3;79:16	save (13)
required (27) 24:17;28:16;33:15,16,17; 36:4,9;37:11;80:11;104:8; 105:1;113:20;115:17; 137:3;138:21;142:21; 143:6;150:11;162:4;176:6, 12;177:14,19;182:2;190:6; 203:7;217:15	restrictions (9) 33:7;139:17;140:1;166:4; 167:1;173:17,18;174:17; 198:6	roles (2) 45:8,12	
requirement (32) 25:4;32:9;33:19;43:21, 21;44:2,5;59:18;71:9;73:9,	rests (1) 183:4	rolling (1) 89:10	
	retire (1) 187:2		

69:17;86:14;95:11,17,18; 100:1,5,7;151:11;206:11, 11,14,16 saving (1) 152:13 saw (7) 131:20;132:3;153:2,5; 158:1;205:5,11 saying (7) 102:13;131:9;164:3; 205:20;210:3;217:2;219:9 scan (1) 35:15 scenario-driven (1) 37:1 Schasteen (2) 65:15,17 schedule (5) 76:12;79:9,14;88:1,4 schoolhouse (1) 175:14 Science (1) 68:2 scientist (1) 68:1 SCIF (3) 180:5;190:18,20 Scott (2) 6:19,21 scrape (1) 137:16 scrapes (2) 82:17,20 screen (1) 9:19 screenshot (1) 14:12 screenshots (1) 14:9 scripts (1) 181:19 scrub (1) 99:2 scrubs (1) 97:18 search (4) 164:4;178:20;179:11; 184:15 searched (1) 185:13 seated (1) 20:19 second (4) 14:11;131:7;188:9;212:1 secondly (2) 25:3;58:19 secret (3) 151:9;152:8,9 secretary (2) 22:4;77:2 section (5) 31:11;52:16;113:3,5; 114:5	sections (4) 31:17,18;126:21;127:2 secure (4) 94:17;95:8;149:19; 165:16 secured (1) 125:9 security (50) 7:16;8:8,13;23:2,6;24:13, 17,17;28:11;40:8,8,19,20, 20;46:1;47:9;51:4,15; 55:11,21;59:13,14;63:7; 64:1;80:15,16,19;81:4,16; 82:3,8,13;102:9,12;109:11, 16;111:21;112:5,5;114:5; 136:7;150:15,20;177:14; 178:9;179:9;181:6,7; 182:18;216:3 security-wise (1) 182:14 seeing (3) 146:12;153:20;222:9 seemed (1) 207:11 seems (1) 131:2 selected (2) 67:21;68:17 sending (1) 64:17 sends (4) 62:20;64:10,10;102:18 senior (1) 144:17 sense (3) 2:17;72:10;73:20 sensitive (1) 53:18 sensor (2) 69:18,19 sent (5) 64:8;101:20;104:15,20, 20 sentence (1) 49:15 separate (3) 13:7;88:21;172:19 separately (1) 30:2 September (1) 188:19 sergeant (9) 166:16;195:9;196:18; 205:17,19;206:19;222:4,7, 21 series (4) 14:21;53:7;75:21;210:7 serve (1) 187:4 server (12) 60:7;68:16;69:7,16; 80:18;83:2;95:20;100:6,14, 16;107:14;189:18	servers (2) 82:9;188:6 serves (1) 25:2 service (9) 22:14;26:4;59:16;97:13; 100:2;101:7;102:11; 104:20;107:11 services (2) 22:14;144:21 serving (1) 24:5 session (3) 12:3,3;224:6 set (12) 72:18;73:19;75:7,13,14; 80:1,2,5,10;137:17;186:8; 217:19 sets (3) 74:16;81:15;84:1 settings (1) 195:1 setup (4) 73:7;79:17,18,21 seven (2) 67:17;128:7 severable (1) 80:3 several (5) 118:20;171:13;180:17, 17;194:11 severely (1) 213:17 share (3) 141:6;151:14;169:16 shared (16) 103:6,10,11,15;137:6; 139:10,21;141:8;151:6,16, 18;165:14;169:14,14,18; 205:2 SharePoint (1) 170:8 Sharing (2) 43:9,9 SHAVEN (10) 4:4;7:3,5,11,13;10:13; 11:18;14:18;19:5,10 shelf (1) 122:20 shift (7) 192:2;205:6;222:5,6,9,12, 14 shifts (1) 222:12 shop (1) 166:13 short (5) 133:10;162:8;164:14; 197:2;213:21 shortcut (1) 103:15 Shortly (1) 196:21	show (2) 119:8;127:5 showed (2) 101:10;147:9 Showing (2) 127:11;177:13 shown (2) 145:14;147:11 shows (4) 12:2,20;155:2;177:18 sic (1) 33:8 side (11) 64:17,18;100:5,6,8,9,10, 11,15,17;217:9 sides (1) 186:9 sign (10) 37:2,3;78:8;115:15; 116:1,4,7,8;143:17;146:4 signal (2) 113:12,13 signals (1) 75:18 signature (2) 30:21,21 signed (33) 113:3;114:3,5;115:19; 117:17,21;119:11,14,18; 120:3,12,13,16;121:17; 122:14;123:11;129:11,14; 130:16;131:6,8,21;132:6; 135:6,19;136:12;138:18; 145:17;146:13;149:4; 163:18;179:9;217:1 signify (1) 25:8 signing (4) 115:7;136:3;146:5;210:3 signs (1) 34:4 similar (20) 40:17;75:10;117:19,20; 118:4,5;130:17,18;131:3,4, 9;135:9,12;138:20;139:1; 145:15;146:11,21;147:8; 193:20 simple (1) 16:14 simplify (1) 172:9 simply (3) 142:20;143:7;162:1 single (1) 29:14 SIPR (3) 115:14;139:16;190:10 SIPRNET (23) 16:2;113:19,21;114:1,17; 115:10,16;119:12;120:1,14; 124:17;136:4;168:15,19,21; 169:2,3,7;170:4;171:5,17; 172:12;174:5
---	--	---	--

sit (3) 28:13;77:1;109:6	59:8;81:8;96:19;97:2,3; 15;116:6,8;120:13;141:9; 143:14,17;144:19;163:2,15; 197:14;214:12;215:20; 216:6;220:13,15,18	194:19;197:5	147:6;192:16;207:2;209:2; 210:8,12;212:9;216:19; 219:14
site (7) 48:17,18,18,19;169:18, 21;170:21		speak (2) 94:21;218:12	standards (5) 23:16;28:7;31:4,4;32:13
sites (5) 54:6;82:17,21;137:16; 169:13	sole (1) 27:2	spec (3) 85:12;86:4,4	standing (1) 26:7
sits (2) 70:6;88:19	solely (1) 56:13	SPECIAL (5) 4:4;7:2,5;14:18;217:1	standpoint (2) 23:15;213:5
sitting (1) 123:3	solid (1) 73:19	specialist (1) 43:19	start (3) 14:20;194:3;219:10
situation (4) 56:20;161:9;220:17; 222:7	solution (18) 44:1;73:8;75:13,16,19; 76:1,3,7,8,13;77:10,13; 79:10,15;81:7;87:11,12; 88:11	specific (10) 31:17;39:20;44:7;53:16; 54:5;130:11;137:18;185:8; 218:4;223:4	started (4) 26:3;68:12;205:12; 210:16
situations (1) 216:10	solutions (5) 74:7;81:4;87:7;88:6; 89:11	specifically (15) 15:7;34:14;35:10;40:15; 53:1,10,11;54:1;84:3; 105:13;144:7;170:15; 171:1;172:3;183:11	starts (4) 85:1;119:2;130:8;163:9
six (4) 67:17;81:13,14;197:6	solve (1) 144:20	specification (3) 38:12,15;121:6	state (3) 49:11;53:6,12
size (1) 207:4	Somebody (14) 15:15;17:2;41:21;46:9, 19;63:8;123:12;125:12; 158:21;168:9;177:2;208:8; 213:20;217:2	specifications (4) 38:9;121:2,3;128:17	statement (6) 54:19;62:2;138:21;139:1; 210:21;217:12
skills (3) 191:1,4,13	somebody's (2) 212:13,17	specifics (1) 99:3	STATES (21) 1:2,4;6:10;7:2;20:13; 21:4;29:16;38:4;40:1; 65:11,19;66:5;97:18;98:2; 108:5,14;110:6;115:6; 124:8;186:6;223:18
skip (1) 207:16	Someone (8) 64:9,10;88:19;109:6; 113:20;141:17;166:10; 180:4	specify (2) 44:6,7	stating (1) 114:3
Slayer (9) 188:2,4;198:17,18,21; 209:5;212:5;218:11;219:4	sometime (1) 112:19	specs (4) 85:12,14;87:4,5	station (1) 80:18
slide (1) 12:13	sometimes (6) 205:13;206:8,13,14,16,17	speculation (1) 17:7	stationed (4) 187:21;188:14;189:19; 198:17
Slightly (1) 145:4	somewhat (1) 70:3	speed (1) 17:21	status (2) 139:13;186:21
small (3) 84:6;96:11;97:3	somewhere (3) 103:18;172:5;206:11	spend (1) 27:15	statutorily (1) 71:21
smaller (1) 75:1	sorry (12) 19:6;40:2;49:18,20; 59:14;60:12;67:12;98:1; 172:10;177:20;194:5; 216:15	spent (2) 27:16;67:17	step (4) 8:8;73:18;74:1;207:16
smart (1) 8:9	sort (13) 55:14;86:9,20;89:7,10; 90:12;94:6;97:8;107:2; 130:13;169:17;183:1;200:3	spite (1) 203:13	steps (12) 73:7,9;192:7,16;193:16; 194:9,18;200:5;203:1; 206:3,4;212:4
SME (1) 36:5	sorts (1) 181:20	splice (1) 184:2	still (11) 7:11;34:10;44:8;56:2; 90:1;96:7;125:4;158:16; 184:3;186:4;203:13
snow (3) 193:12,13;204:8	sound (1) 209:15	spoke (3) 83:14;94:16;96:3	stipulated (5) 6:16,18,21;65:17;108:12
software (62) 35:13;41:16,18;42:5,15, 18;43:6,14;44:7;46:13; 47:7,17;48:7;60:12;68:20; 71:16;73:7,9;75:5;78:3,6; 81:7;84:11,21;88:14;89:5; 91:10,18;92:10,12,14,16, 19;98:8;99:14;103:9,10,17; 136:15;137:1;138:6; 140:16,21;141:4,15,18,19; 142:1,7;143:21;144:3; 161:2,4;162:5;163:19; 188:8;198:19;208:3,10; 209:4;220:14,16	Sounds (1) 176:5	spray (1) 203:10	stipulation (4) 65:12,14;108:6,9
soldier (19) 57:8,10;98:1;155:15; 164:19;165:3,5,9;166:10; 179:21;194:15;198:10; 199:7;200:13;214:4,8; 215:6,12,15	source (2) 87:18;144:4	spreadsheet (1) 48:4	stipulations (2) 6:11;224:7
soldiers (22)	sources (1) 137:16	spreadsheets (2) 45:11;181:20	stone (1) 72:18
	space (5) 69:18;86:2;193:5;196:8; 207:10	stack (1) 194:19	stop (9) 9:21;16:7;103:2;159:17; 160:5,9,12,13;216:15
	spare (2)	staff (9) 22:4;55:21,21;56:1,15, 15;157:7,10;166:10	stopped (1) 210:15
		staffing (1) 27:3	stops (1) 180:4
		stage (2) 90:13;196:20	
		stand (3) 66:6;93:9;109:6	
		standalone (2) 23:4,5	
		standard (13) 37:15;55:9,15;61:18;	

<p>storage (2) 140:7;152:3</p> <p>store (7) 69:17;139:11;151:8,14; 152:7,9;193:10</p> <p>stored (9) 57:16;58:16;60:7;122:16, 19,20;152:6;193:14;204:4</p> <p>Storing (6) 8:8;60:3,3,5;204:2,13</p> <p>stressing (1) 77:18</p> <p>string (4) 15:9,12,16,19</p> <p>struggling (1) 71:1</p> <p>studies (1) 89:17</p> <p>studying (2) 89:20;90:2</p> <p>stuff (6) 91:9;157:11;164:11; 165:2;174:3;214:4</p> <p>sub (1) 89:8</p> <p>subject (4) 24:5;56:3;74:10;135:11</p> <p>submit (4) 175:21;176:7,12;177:1</p> <p>subparagraph (2) 138:14,19</p> <p>subparagraphs (1) 31:14</p> <p>subsequent (1) 27:7</p> <p>substantial (1) 147:11</p> <p>substantially (2) 118:3;120:18</p> <p>successful (2) 12:21;77:14</p> <p>successfully (2) 12:5;162:9</p> <p>suggest (1) 11:2</p> <p>suggestions (4) 215:10,11,12,16</p> <p>suit (1) 127:3</p> <p>suitability (1) 78:15</p> <p>suitable (1) 77:20</p> <p>suite (2) 190:5;217:14</p> <p>suites (2) 69:7;145:1</p> <p>supervise (1) 146:4</p> <p>supervisor (11) 43:20;56:19;57:9;114:3; 157:13;159:7;165:6; 173:20;174:18;215:13,16</p>	<p>supervisors (2) 44:21;173:16</p> <p>support (12) 24:2;26:6,6;34:11;43:18; 58:4;69:7;70:11,14;74:20; 86:2;189:17</p> <p>supporting (2) 26:11;69:9</p> <p>supports (1) 86:7</p> <p>supposed (6) 176:16;177:10;178:3; 198:19;220:10;221:11</p> <p>Sure (26) 11:20;12:15;35:20;37:7; 57:2;58:13;60:17;91:17; 94:8;98:6;106:12,13,15; 108:4;126:13;134:12; 145:10;167:18;168:16,20; 178:4;208:4;213:1;218:8; 222:11,15</p> <p>Surely (1) 121:12</p> <p>surfaced (1) 56:9</p> <p>surrounding (1) 48:1</p> <p>Surveillance (1) 66:18</p> <p>survivability (1) 78:15</p> <p>survivable (2) 77:20;80:21</p> <p>suspect (1) 40:11</p> <p>sustain (1) 132:9</p> <p>sustainable (1) 78:17</p> <p>sustainment (1) 93:15</p> <p>swapping (1) 216:16</p> <p>sworn (5) 7:7;21:8;66:9;110:10; 186:14</p> <p>symptoms (2) 192:18;193:1</p> <p>system (138) 7:16;8:12,16,16,19;9:3,5, 7,11;10:1,4;11:3;12:1,19; 13:4,11,13;16:10,14;19:19; 25:16;31:3,6;32:10;33:1,2, 12,13;34:9;35:11;41:16,20; 42:11,12,16;43:3,19;44:3, 11,14,14;45:7,9;46:2,5,15, 21;47:8,12,16;48:8;50:5,18, 19;52:13;57:17;58:16;60:3, 3,4,15,16;61:5;62:3,10; 64:2,5,7;66:19;67:16,19; 69:2;73:11;77:18,18,19,20; 78:10,16;79:17,18,21;80:1, 3,9;82:13,14;83:6;84:10,10,</p>	<p>12;85:18;92:2,6,7;93:16,20; 96:2,4,4;97:5;98:5,8,9,19, 21;99:2,4,5,6,8,9,11;100:11, 12;102:6,10;103:9,16; 104:5,5,7;111:12;136:16; 137:5;140:20;141:5;168:2, 7,9,12,13;190:15;193:21; 196:9;200:7;216:3;217:19</p> <p>systematic (2) 7:14,14</p> <p>systems (37) 22:21;23:1;24:13;25:13; 28:18;31:2;34:16;35:15; 51:5,13;67:4,19;68:14,19; 69:5;70:9;72:19,21;74:12; 75:17,20;76:19;80:17; 81:20;82:5;89:1,7;99:14; 101:21;111:1,20;112:5; 145:1,2;167:12;171:1; 176:18</p>	<p>11,12;165:2,15,18;166:2,7, 8;167:2;170:9;180:13,16; 181:9;182:5;184:12,20</p> <p>team (9) 22:2,5;26:5,6,20;68:12; 70:11;87:10,10</p> <p>teams (7) 71:17,18;74:5,6,9;86:21; 87:2</p> <p>technical (15) 40:20;68:17;71:13,14; 75:15;79:9,13;101:6;102:8, 10,13;105:6;172:16; 173:18;174:16</p> <p>technically (2) 59:12;217:20</p> <p>technicians (1) 144:19</p> <p>technology (8) 24:7;44:17;45:13;51:7,8; 67:3;68:2;72:8</p> <p>teeth (2) 54:18,20</p> <p>telephone (1) 40:19</p> <p>Telling (3) 192:2;200:4;220:21</p> <p>template (1) 118:12</p> <p>temporarily (6) 20:10;65:5;107:20,21; 186:2;223:14</p> <p>Temporary (9) 20:8,9;65:3,4;107:19; 185:21;186:1;223:12,13</p> <p>ten (1) 20:16</p> <p>term (7) 82:1;83:18;96:7;97:4; 99:2;147:19;171:10</p> <p>termed (1) 72:19</p> <p>terms (20) 2:16;69:14;70:3;76:21; 79:18,21;80:21;81:3,17; 89:11,11;118:10;119:21; 126:11;128:19;130:10; 131:4,12,13,15</p> <p>test (12) 37:8;73:21;77:11,12,12, 15,16,17;78:5,13;91:5; 109:16</p> <p>tested (3) 95:5;218:9;219:19</p> <p>tester (2) 86:4,7</p> <p>testified (12) 7:8;19:12;21:10;66:11; 110:12;142:15;144:12; 180:21;182:4;183:10; 186:16;201:14</p> <p>testify (2) 122:1;132:5</p>
		T	
		<p>table (5) 17:13,14,16,17;18:1</p> <p>tables (1) 18:4</p> <p>tactics (1) 192:21</p> <p>tailored (1) 18:4</p> <p>talk (25) 26:14;30:15;35:18;41:3, 5;45:15;53:6;72:15;73:6; 77:21;82:15;115:18; 132:10,14;140:12;145:13, 14;154:7;157:11;165:13; 167:4;168:14;191:2;197:9; 202:10</p> <p>talked (10) 17:14;52:20;54:16;84:20; 94:16;146:11;172:19; 180:13;191:7;205:1</p> <p>talking (3) 121:11;157:20;222:18</p> <p>talks (1) 12:1</p> <p>tampered (1) 181:4</p> <p>target (1) 135:2</p> <p>task (2) 87:5;179:8</p> <p>tasks (3) 48:8;85:20;86:1</p> <p>taught (1) 73:2</p> <p>T-drive (45) 139:7,9,10,13,18;140:4,5, 10;151:6,8,12;152:1,6,10; 153:3,21;154:5;155:9; 156:3;158:2,6,9,20;159:5, 13,16;160:17;163:5;164:4,</p>	

<p>testifying (1) 146:17</p> <p>testimony (16) 2:18;6:16,19,21;61:19; 65:6,14,17;106:20;108:1,6, 9,12;121:19;223:15;224:7</p> <p>testing (4) 91:1,7;94:9;109:12</p> <p>tests (2) 77:15;218:10</p> <p>textbook (1) 178:5</p> <p>theater (2) 92:10,11</p> <p>theaters (1) 26:9</p> <p>third (1) 111:21</p> <p>THOMAS (5) 3:13;5:4;108:15;110:7,9</p> <p>though (7) 55:17;131:7;158:5; 164:10;174:21;201:6; 217:19</p> <p>thought (3) 106:18;164:1;201:21</p> <p>thousands (1) 169:7</p> <p>threat (3) 53:12;159:21;181:6</p> <p>threats (10) 40:4,9,9,11,13,15;41:3; 45:16;52:21;53:3</p> <p>three (8) 79:11;111:19;119:7; 121:2;128:17;161:8; 176:21;196:1</p> <p>three-month (1) 174:1</p> <p>three-sided (1) 109:8</p> <p>threshold (2) 84:2,7</p> <p>throughout (6) 35:9;61:17;79:7;118:10; 123:2;188:6</p> <p>thumb (2) 142:19;150:19</p> <p>times (11) 38:2;51:6;56:16;63:2,16; 83:19;157:8;194:12; 195:19,21;197:1</p> <p>tinker (2) 96:20;217:21</p> <p>today (10) 22:5;70:10;76:17;77:1; 96:19;97:3,14;123:16,17; 137:12</p> <p>together (1) 156:20</p> <p>token (1) 60:13</p> <p>told (8)</p>	<p>57:8;159:12,15;163:21; 173:8,10,20;221:10</p> <p>Tom (2) 110:14;172:17</p> <p>tomorrow (1) 224:10</p> <p>tonight (1) 224:11</p> <p>took (7) 2:6;29:19;134:11;154:12; 189:2;192:7;194:9</p> <p>tool (9) 209:2;210:13,16;211:7,7, 9,13,15;212:9</p> <p>tools (12) 15:20;47:11,13,17,19,21; 48:1,5;96:8;190:5;217:15; 219:13</p> <p>TOOMAN (18) 3:12;48:21;49:4;50:1; 52:3,4;57:13,14;59:19; 61:13;65:2;83:10;95:17; 99:19;104:13,14;105:10; 106:1</p> <p>top (3) 24:16;84:6;204:10</p> <p>topics (1) 112:1</p> <p>totally (2) 67:15;98:4</p> <p>touch (1) 98:8</p> <p>towards (1) 124:21</p> <p>trade (6) 71:15;74:11;75:8,9,10; 89:17</p> <p>Traditionally (2) 46:4;61:3</p> <p>train (2) 78:3,8</p> <p>trained (1) 61:7</p> <p>training (49) 35:19;36:1,5,8,9,10,13, 15,17;37:1,5,10,12,14,14, 17;38:1,6,7,13,14;39:4,7, 16;40:5,6,7,14;52:21;53:1, 2,4,7;54:4,11;62:16;74:11; 111:4,9,18;114:8,16,19,20; 150:12,15,16;151:1;168:12</p> <p>transcript (3) 2:3,11,14</p> <p>transfer (1) 195:6</p> <p>transferred (1) 222:19</p> <p>transition (1) 93:13</p> <p>translated (1) 2:15</p> <p>treated (3) 50:20;60:19,21</p>	<p>trial (4) 65:7;108:3;119:5;186:4</p> <p>tried (7) 72:18;103:1,14;182:17; 184:2;193:2;222:11</p> <p>tries (3) 63:12;79:5;88:20</p> <p>Trojan (2) 67:14,18</p> <p>troubleshoot (2) 192:18;219:13</p> <p>troubleshooting (3) 192:20;194:17;206:2</p> <p>true (8) 54:19;58:21;62:2;72:18; 95:4;103:5;203:20;214:10</p> <p>trust (9) 169:15,20;170:6;171:7,8, 9,10,13;202:1</p> <p>trusted (1) 179:14</p> <p>truth (15) 7:7,7,8;21:9,9,10;66:10, 10,11;110:11,11,12;186:15, 15,16</p> <p>try (5) 85:8;104:8;121:15;172:9; 206:7</p> <p>trying (6) 40:16;77:6;161:10; 172:11;177:21;216:11</p> <p>turned (2) 16:5;124:3</p> <p>turns (1) 98:7</p> <p>two (18) 6:11;8:11,14;14:9;25:1; 27:7;39:3;60:19;72:14; 88:8;119:7;128:14;133:12; 183:5;203:19;204:4; 216:15;222:4</p> <p>type (12) 8:3;47:7;102:21;114:12, 16;137:18;143:21;152:5; 157:10;170:20;187:11; 189:15</p> <p>types (3) 86:3;168:3;184:16</p> <p>typical (2) 223:6,7</p> <p>Typically (2) 90:15;91:19</p>	<p>unable (1) 116:17</p> <p>unacceptable (1) 182:13</p> <p>unaccredited (1) 43:6</p> <p>unauthorized (22) 35:10;41:18;43:5;46:9, 20;99:14,15;136:6;143:15, 18;153:2,8;159:5,13,16; 160:17;164:18;178:21; 179:10;180:21;182:6; 183:16</p> <p>uncertified (1) 2:13</p> <p>uncommon (1) 223:8</p> <p>under (11) 7:11;56:20;60:19;76:12; 115:8;131:13;134:13; 144:8;165:2;175:17;183:11</p> <p>underneath (2) 22:7;203:14</p> <p>understood (7) 97:21;101:11;104:16; 149:18;164:20;201:21,21</p> <p>unedited (1) 2:13</p> <p>unencrypted (1) 165:19</p> <p>unique (3) 15:9,16;25:6</p> <p>unit (32) 52:16;55:7,18;77:11,18; 78:4,7;92:1,5;93:19;94:2,5, 8;97:7,9,17;98:4,9,11; 101:16;124:7;127:3; 130:11,12;163:15,15;171:4; 184:2;188:20;189:2; 216:18,20</p> <p>UNITED (19) 1:2,4;6:10;7:2;20:13; 21:4;22:19;29:16;38:4; 40:1;65:11,19;66:5;108:5, 14;110:6;124:8;186:6; 223:18</p> <p>units (10) 92:11,15;101:21;171:7; 180:15,17;189:17;210:15; 214:17;216:16</p> <p>universal (1) 195:5</p> <p>unknowingly (1) 56:2</p> <p>unless (10) 123:4;165:20;166:9; 169:19;171:1;175:1;181:4; 185:17;196:5,16</p> <p>unplugged (2) 160:14;164:13</p> <p>up (38) 8:11,14;9:9,19;12:13; 13:11;17:21;25:16;29:3;</p>
---	--	--	--

<p>40:19;51:8;68:13;71:20; 80:1,2,5,10;85:12;88:17; 93:9;98:4;103:13;107:9,10; 109:13;140:7;151:8;152:7; 162:3;165:7;169:1;170:21; 190:9;195:2;204:10; 217:19;222:1,7 update (3) 93:6;98:18;102:9 updated (2) 98:12;103:20 updates (2) 91:18;216:2 updating (2) 98:16;99:5 upgrade (2) 92:12;185:7 upload (1) 58:20 uploading (1) 35:15 upon (25) 25:17;47:3;51:5;57:11; 75:7;77:14;84:2;85:18; 89:4;99:7;116:6;117:8; 121:9;126:9;146:17;147:2; 160:3;171:21;184:9; 205:14,19;210:19;211:21; 216:5,9 URL (1) 170:20 usability (1) 23:2 USB (3) 60:13;194:1;195:4 use (71) 9:4;13:14,18;15:21; 17:15;18:1;23:8;30:16,18, 19;31:2;32:7,21;33:2,13,20; 34:9,9,16;35:11,14;39:5; 41:16;42:17;44:7,11;45:2,7, 9,12;54:5;78:4;85:5;96:7, 16;99:2;102:3;104:17; 114:15;115:5;117:3;119:4; 120:1,10;124:9;126:4; 127:9;128:3,13;129:7; 130:5,9;132:19;135:10; 143:20;147:6;150:19; 151:19;156:11;161:4; 162:5;167:4,14;182:17; 185:6;190:6;203:7;209:2; 211:13;217:20;219:13 used (29) 34:1;37:15;39:18;41:21; 45:3;47:6;49:19;74:17; 78:9;83:18;95:14;100:17; 117:8;119:15,20;126:7,10, 12;128:15;129:10,11; 134:11,17;137:15;138:6; 204:7;212:21;217:15;219:5 user (85) 7:17;8:17;17:11;18:13, 14,15;20:2;34:3,4,11;36:4,</p>	<p>14:40;7,7;41:17;43:2,10,15, 16,17;45:2,3,4,6;46:3,10; 47:5,19,21;48:20;50:5;51:6, 9,9,16,18;54:7;57:3,3;60:8; 61:1,16,20;62:2,8,19;63:3, 12;64:3,11;74:11;82:12; 92:1;100:8,10,12,13; 102:20;103:2,11,20;107:3, 12,16;140:3;141:1;143:4; 151:13,15;165:20;167:13; 170:14;192:16;193:6; 198:2;200:21;201:5,19; 204:14,16,19;208:20; 213:16;215:8;219:15 users (39) 8:18;17:5;28:14;30:20; 31:5;32:12;36:12;39:6; 40:11;42:4,17;44:6;45:20; 51:3;61:3,4;62:17;63:11; 82:11;139:11;140:9; 151:11;158:8;167:3; 170:10;171:8;189:19; 193:10;203:19;204:1,2,4, 13;222:4,14,15,18,19;223:7 users' (1) 32:11 user's (5) 18:4,13;44:10;204:16; 206:16 uses (10) 31:21;32:20;54:11,14; 82:17;94:18;100:1;104:5; 130:10;173:21 using (21) 13:8;17:1;23:16;47:1; 77:18;118:12;143:3,15,18; 168:9;174:18;175:3; 200:11,20;201:2;202:17; 210:15,16;217:10;219:10, 11 Usually (13) 33:11;43:2;53:6;56:9; 64:13;92:11;123:8;193:18; 198:18,20;203:18;207:2,15 utility (4) 10:7,18,19;12:7 utilized (1) 13:6</p>	<p>validating (1) 77:19 value (13) 8:7,10;15:4;17:19,20; 18:3,7,8,11;19:12,14,18,21 values (2) 17:15,17 variations (1) 61:8 variety (1) 40:10 various (1) 96:13 vary (1) 147:14 VAT (1) 184:16 VBS (1) 184:16 verbatim (7) 2:11;118:1;126:19;127:1, 1,135:21;136:14 Verification (2) 12:4;170:1 verify (1) 16:2 verifying (2) 114:5;175:16 version (26) 27:5,6,12;33:18;39:9,9, 11,21;68:15;104:18; 128:12;185:7,7;218:4,9,20; 219:7,8,10;220:1,3,5,9,9,13; 221:2 version-based (2) 218:7,18 versions (13) 27:7,9;36:7;39:8,17;53:4, 5,9;128:14;218:12,13; 219:18;220:18 vetted (2) 83:15;219:19 VI (1) 1:1 via (1) 73:21 video (4) 64:10,17,18;165:18 videos (1) 54:10 view (14) 9:2,8;13:9,14,17,20;17:1; 55:4;76:20;140:2;166:17; 172:7,18;173:4 viewed (2) 13:6;159:20 viewing (1) 14:12 violate (1) 43:3 violating (4) 31:16;34:20;50:2;128:18 violation (5)</p>	<p>63:4,7;128:17;184:4,5 violations (6) 35:8,10;51:14;121:5; 181:7;183:21 Virginia (2) 21:12;186:19 virtual (7) 16:5,7,8,10,17,17,19 viruses (1) 40:12 visitors (3) 171:2,2,3 Vista (1) 112:6 VLC (1) 184:18 VOIR (8) 5:6,8;119:6,9,10;124:12, 15;127:7 VOLUME (1) 1:1 Von (47) 3:8;21:3,4,11;29:1,4,16; 30:12,14;31:7,10,20;32:3,6, 15,17,19;35:2;38:4,11,16, 19;39:1;40:1,3,21;41:2,10; 49:9,17;50:4,10,13;51:20; 60:1;61:12;65:1,4;66:5,12; 83:7;99:21;100:20;104:12; 106:2;107:18,20 VonElten (1) 41:7 VS (1) 1:5 VTC (1) 144:21 vulnerabilities (3) 42:13;80:21;81:1</p>
W			
<p>waivers (1) 56:12 waking (1) 179:12 walked (1) 185:17 WAN (1) 144:21 wants (3) 101:19;102:18;128:13 war (3) 72:1;79:2,3 Warfare (1) 66:18 warning (3) 32:10,14;33:3 Warrant (2) 6:14,16 warrants (1) 170:13 watching (1) 2:7</p>			

way (22) 9:2;12:16,17;15:18,21; 39:7;46:6,15;50:14;68:13; 70:10;82:12;93:1,2,5;98:9; 154:19;163:11;207:12; 213:12,15,20	Whereupon (9) 6:15,20;7:4;21:6;65:16; 66:7;108:11;110:8;186:12	86:10;87:9,18;88:2,7; 181:20	
ways (4) 46:10,12;59:12;92:19	wherever (1) 189:20	worded (1) 126:19	0
weapon (2) 78:9;182:19	Whiskey (1) 187:8	wording (1) 32:8	0930 (1) 224:12
weather (1) 224:9	White (2) 108:10,12	word-of-mouth (1) 198:20	1
WEAVER (20) 4:7;21:5,7,12,14;22:17; 29:7;30:15;31:11;39:2; 41:12;47:11;48:11;49:10; 51:16;52:5,7;57:15;59:19; 60:2	whole (10) 7:7;21:9;48:19;66:10; 93:2;110:11;121:11;151:2; 162:6;186:15	words (2) 134:12;166:6	1 (7) 69:1;71:3;73:1;77:4; 83:19;84:12;88:8
web (9) 34:11;36:18;39:15;82:17, 21;83:2,9;5:15,19,20	Whose (1) 45:2	work (22) 26:19;37:16;45:10;48:13; 66:15,16;77:20;78:16,16; 79:2;96:16,19,20;97:6,12; 171:6;184:3;187:11; 190:17;194:20;222:13; 224:8	1:30 (1) 1:16
website (2) 36:21;48:16	WHYTE (42) 3:7;21:3;110:13;120:15, 17;121:19;122:7,10;129:15, 16;130:19;131:18;132:13, 17;133:4,20;134:1,4,6; 135:4;139:3,5;144:10,11; 145:11;178:12,14;180:8; 183:5,8;184:7;185:11,12; 186:1,6,17;192:6,11;202:3; 221:16;223:11,13	worked (8) 67:11,14;68:8,13;141:9; 174:1;222:5,6	10 (3) 6:19;37:6;108:10
Wednesday (1) 1:16	wider (1) 75:20	working (8) 22:2;25:19;26:1;67:18; 68:4,6;92:7;224:6	100 (1) 207:21
week (2) 164:16;224:12	WikiLeaks (1) 54:12	works (4) 8:2;76:20;81:13;98:7	101 (1) 4:17
weeks (1) 112:15	Windows (4) 16:9,11;112:6;181:15	world (2) 111:5;171:5	1030 (1) 128:18
weight (2) 131:10;204:11	within (18) 7:16;15:10;23:2;24:18; 25:4;26:9;28:21;34:15; 36:6,12;37:12;52:21;71:2; 112:14;147:15,18;170:15; 177:11	worry (1) 218:16	104 (3) 4:18;38:11,15
welfare (2) 58:5;59:7	without (17) 42:5;46:17;48:8;56:2; 80:2,5;105:17;137:2;141:1; 147:21;148:9;149:7;154:9; 186:8;198:5;201:6;222:18	Worth (1) 111:14	106 (1) 4:19
Wells (1) 70:19	WITNESS (51) 4:4,7,13;5:4,17;6:8;7:6; 10:10;11:7;14:3;17:9; 20:12;21:8;29:5;30:13; 49:3,5;65:9;66:9;105:7; 108:4;109:6,7,9,11,13,14, 19;110:5,10;121:20;122:1, 7;124:13;128:9;129:4,17, 21;131:1,7;132:11,14,20; 133:20,20;134:20;135:16; 136:10;138:15;186:14; 223:17	worthiness (4) 138:2,4,5,9	107 (2) 108:8,11
weren't (5) 145:21;146:8;167:16; 215:19;219:14	witness' (1) 109:14	worthless (1) 96:6	10-minute (3) 20:14;108:16;223:19
Wget (50) 48:11,14,20;49:1,5; 51:17;61:21;62:3,10;82:15, 15,16,17,17;83:3,5;94:16, 17,20;95:14;100:15,17; 102:21;104:2,6,7,7;105:20; 106:3;137:10,14,20;138:8; 142:16,17;143:1,4,9,11,21; 155:10,13,15;163:8,12; 199:4,7,10;201:8,11	witnesses (1) 20:15	wrapper (2) 107:7,16	10th (5) 92:6,7;136:4;139:20; 169:10
whatnot (3) 126:11;147:20;214:20	WMOR (1) 58:4	write (3) 27:5;213:16;214:1	10-year (2) 121:5,6
What's (22) 11:9;13:16;16:7;17:3,8, 13;55:5,6;59:5;60:2;81:7; 85:14;90:4,5;95:16;98:15; 104:2;105:1;127:11; 175:21;177:19;178:7	word (19) 2:16;13:17,18;74:18,19, 19;75:3,4;85:6,8,16,18,21;	Writing (1) 12:3	11 (1) 121:6
whenever (6) 107:8;158:1;165:3;206:7; 218:2,17		written (2) 47:3;181:19	110 (1) 5:5
whereas (1) 8:17		wrought (1) 58:19	112 (2) 11:10,19
wherein (1) 209:18			114 (3) 65:20,21;66:3
		X	117 (3) 6:11,13,15
		X86-1.3.5 (2) 12:1,20	119 (3) 5:6;6:12,20
		XP (1) 7:16	12 (4) 1:16;4:2;5:2;89:4
		xxx-xx-9504 (1) 1:7	122 (1) 5:7
		Y	124 (1) 5:8
		year (5) 36:5;68:2;84:3;93:12; 127:15	125 (5) 10:9,11;11:17;12:11;19:7
		years (9) 28:3;39:16;67:7,17;68:9; 72:14;176:21;180:17;187:6	129 (2) 5:9;12:4
			13 (3) 24:10;67:7;69:5
			130 (5) 14:2,4;18:20,21;19:2
			1317 (1) 11:21
			1400 (1)

20:17 145 (1) 5:10 1-5J (3) 34:13,14;35:7 16 (1) 89:4 17:48:51 (1) 12:19 178 (1) 5:11 18 (4) 91:19;92:8,13;188:13 180 (1) 5:12 1825 (1) 223:20 183 (1) 5:13 184 (1) 5:14 185 (1) 5:15 186 (1) 5:18 19*7 (1) 21:18 1998 (1) 25:21 1st (3) 11:20;112:11;170:19	2013 (7) 1:16;4:2;5:2;6:19;65:15; 108:10;146:16 202 (1) 5:19 21 (2) 4:8;187:6 210 (8) 120:13;189:4,5,14; 197:14;209:12;212:9; 214:16 210th (3) 112:9;210:14;214:17 22 (5) 14:13;15:5,10;18:16; 41:11 221 (1) 5:20 22211 (1) 1:11 23 (1) 29:11 24 (2) 92:8,13 24/7 (1) 22:2 24-month (1) 91:19 25-1 (1) 27:13 25-2 (14) 27:11;31:17,21;33:18; 58:15;60:19;62:15;128:13, 17;135:6,9;136:13;147:12; 183:12 26 (1) 32:17 2nd (9) 12:18;112:9,20;136:4; 139:19;145:18;149:16; 169:10;180:19		82nd (5) 189:1,2;196:21;210:14; 212:2 83 (1) 4:15
		4	
		40 (3) 15:5,10;18:16 403 (1) 131:13 4-17 (1) 50:2 4-17A (2) 49:10,21 4-5A4C (1) 45:18 49 (2) 119:4;132:18 4-A3 (2) 41:14,15	
		5	
		5,000 (2) 69:7;82:9 50 (1) 115:20 5002 (2) 71:7,8 52 (1) 4:9 53 (3) 111:7,10,11 58,000 (1) 69:8	
		6	
		6 (1) 136:9 6:22 (2) 224:19,21 6:25 (1) 223:21 60 (1) 4:10 61 (3) 4:11;119:2;130:8 66 (1) 4:14	
		7	
		7 (4) 4:5;38:20;39:9;41:1 700 (2) 69:6;82:9	
		8	
		8 (3) 12:10;39:9,21 80 (2) 65:13,16 80C1104 (2) 15:1;18:7	
2			
2 (3) 71:4;84:6;121:3 2:00 (1) 20:17 20 (2) 37:7;74:3 2000 (1) 39:9 2001 (1) 25:10 2002 (1) 26:19 2003 (3) 27:7,14;28:3 2005 (1) 187:3 2007 (3) 27:7;28:3;187:18 2008 (1) 105:7 2009 (11) 27:8,10;29:11;33:21; 37:13;112:11;146:14,17; 187:20;188:11,19 2010 (5) 11:20;12:9,18;124:21; 127:16 2011 (2) 23:20;68:7	3		
	3 (7) 11:16;68:15;71:4;84:6,6; 121:3,4 31st (1) 187:3 33 (1) 187:8 35 (1) 190:13 365 (2) 12:12,18 382 (1) 12:20 3A2 (4) 158:12,15,17,19 3rd (1) 170:19		
			9 (1) 65:15 9:30 (1) 224:19 93 (4) 29:17;30:11;41:11;51:21 94 (14) 119:1;129:1,7,17;130:20; 132:20;133:5,6;134:5; 135:15;139:4;148:18,19; 149:13 95 (1) 29:2 99 (1) 4:16